Universidade de Brasília
Instituto de Relações Internacionais

RICARDO ANTONIO PRAVIA JÁCAMO

First steps in the study of cyber-psycho-cognitive operations

DISSERTAÇÃO

Brasília
2019

A mamá, papá y abuelita, porque cada desafío lo enfrenté con mis memorias de su incansable lucha. Sus vidas han sido ejemplo; la mía será muestra de eterna gratitud.

ACKNOWLEDGEMENTS

Shortly after graduating from Macalester College, I departed from an incipient career in the social sciences to explore the field of information technology. Although the economic pressures imposed by my home country's job market would eventually play a part in reinforcing the seemingly permanent character of my decision, its catalyst was a genuine interest in nourishing a "knowledge seed." I owe international studies professor Ahmed Samatar for planting this seed in the spring of 2005, when he introduced my senior seminar colleagues and me to Manuel Castells' "The Information Age" trilogy, which oriented my first extensive study of informationalism and the information society. Computer science professor Elizabeth Shoop and mathematics professor Karen Saxe helped this seed germinate the following semester, teaching me the programming languages underlying the World Wide Web's data dynamics and the fundamental tools for applied calculus. The following fourteen years have seen the seed grow into a tree of knowledge, bearing the signs of a career marked by the study and practice of digital marketing.

To be sure, the list of authors and practitioners that have contributed to this chapter in my professional life is long—to the point that I could hardly avoid leaving people out if I were to take on the task of making a list of all the people and organizations that directly or indirectly contributed to my research. Such list would certainly include the works of Karl Wiegers on software requirements, Alistair Cockburn on software use cases, and Louis Rosenfeld's and Peter Morville's analysis of the World Wide Web as a system of information architectures. Justin Cutroni's and Avinash Kaushik's writings on web analytics would also rank high on the list, as would do the organizations that provided me with the projects to put my knowledge into practice—Progressive Technology Project, avVenta, Internexo, National Instruments, Oxfam and MiWeb, to name a few. Defined in these terms, I would fail to do justice to the large collection of dissertation contributors from the IT and digital marketing industries. Suffice to say that their knowledge paved the way for me to partake of the global endeavor behind the incorporation of detailed explanations of techno-communicational mechanisms in the analysis of current sociopolitical phenomena.

Yet I am only able to join this collective tour de force thanks to a mindset that I cultivated with the help of some of my favorite professors at Macalester: Amparo Menéndez-Carrión, John Guidry, Galo González, Michael Griffin and Cristina Lopez. Their rigorous emphasis on the critical application of theory to the analysis and interpretation of facts as a requirement for the articulation of scientific knowledge laid the solid underpinnings of a Weltanschauung based on critical thinking. This would guide my passage through the digital marketing industry and would allow me to grow intellectually despite the constraints imposed by the operation-driven nature that can characterize its work environments. This pattern stands somewhat at odds with the disruptive character of ICT innovation itself—a characteristic that would play a critical role in my academic career.

At some point before the end of the 2000s, I realized that the technologies that I had been crafting marketing campaigns with were rapidly becoming platforms for the automated construction of dynamic, user-oriented, "ever-relevant" information consumption experiences capable of decisively influencing individual and collective behavior. Then came the so-called "Arab Spring," sparking a years-long global wave of fluid social movements that would push for substantial reforms in their countries' social, political and economic orders. One of their most salient common denominators was said to be the use of social media and other ICTs for the searching, making and sharing of information about "the national reality." After observing the catalyzing effects of these political narratives, it became clear to me that the capabilities of the systems that I had been working with on a daily basis had been instrumentalized to ignite and propel types of phenomena that had been among my primary interests as a social science student.

Nevertheless, regardless of the vast amounts of literature that the social sciences produced on related subjects, I was unable to find works providing detailed explanations of the actual ICT mechanisms underlying the phenomena under discussion. Thus, through the sharing of instruments that are vital to their development, digital marketing and cyberspace-born social movements converged in global history. This had a direct impact in my own trajectory, for it also symbolized a convergence between what was my profession at the time and the vocation that I had longed to exercise. Years later, this intersection between the professional and the academic would give birth to the project proposal that opened the doors of the University of Brasilia for me.

The University's Institute of International Relations has been my "academic home" for the past two and a half years. My project proposal grew into a full-fledged dissertation thanks to a multi-stage review process headed by my research advisor, Alcides Costa Vaz. Other professors also provided feedback and guidance along the way, having considerable impact in the research's development as a whole: Antônio Carlos Lessa, Danielly Silva Ramos Becard, Michelangelo Giotto Santoro Trigueiro and Antônio Jorge Ramalho. Along with professor Ramalho, computer science professor Jorge Fernandes integrated the panel that examined my work; their feedback led to minor, yet important modifications to the text that was originally submitted for evaluation. Last but not least, I wish to thank the head of the Institute's postgraduate program, Ana Flávia Barros-Platiau, as well as the Institute's administrative staff. Their support was simply crucial to my successful completion of the program.

CONTENTS

1. INTRODUCTION

1.1. PRELIMINARIES

Instead of ushering in a smooth power transition process, the American presidential election of 2016 culminated in an official declaration of state of emergency; a denunciation that would equate the outcome of such political contest to the effect of a foreign intervention in the domestic affairs of the U.S. The charge: Moscow articulated an Advanced Persistent Threat (APT) to steal large volumes of voter data, electronic documents and emails from top Democratic Party officials. Moreover, these were later used as part of a micro-targeted political campaign whose objective primary was to prevent candidate Hillary Clinton from winning the election (Alperovitch, 2016; McCain, 2017; Lemay *et al.*, 2018). According to the accusation, the campaign effectively swayed voters in favor of candidate Donald Trump in key electoral battlegrounds, being a decisive factor in his ultimate victory. Before any multilateral examination of the evidence could take place, Washington declared this to be an interference on par with an act of foreign aggression; potentially tantamount to an "act of war," as some analysts and State officials seemed to suggest in articles, press conferences, interviews and even Senate hearings (Arkin *et al.*, 2016; Chotiner, 2016; McCain, 2016; Sanger and Savage, 2016; Szoldra, 2016; McCain, 2017; Greenwald, 2018). It swiftly followed suit: retaliated by imposing diplomatic and economic sanctions that amounted to what could be considered a responsive act of aggression against Russia (United States, 2016c). Mainstream media was quick to frame the sequence of events as "a cyberwar in the making." Yet, no analyst came to the forefront in any capacity to at least point out that, by imbuing the "foreign-intrusion-through-digital-marketing" political narrative with objectivity through consequent retaliatory actions, the U.S. had more than just completed the prelude to a new chapter in the history of Russian-American belligerence.[1] It had in fact "constructed" a new type of casus belli[2].

[1] Ideally, analysts should have questioned the extent to which acts such as publishing an interview between John Pilger and Julian Assange on RT's YouTube channel could be equated to the type of "foreign intrusion" that Immanuel Kant had in mind when he wrote "Perpetual Peace: A philosophical sketch"

[2] Although psychological operations are all but a new type of phenomenon, the case of the American election of 2016 does show some distinctive characteristics; indeed it may be hitherto the only

Over the course of the past two years, fields such as history, political science, sociology and communications have made important contributions to the study of these events from a historical perspective (Patterson, 2016c; b; a; Denton, 2017; Kennedy *et al.*, 2017; Sides *et al.*, 2017; Entman and Usher, 2018) and studies on their political consequences at the international level are in no shortage either (Fidler, 2016; Wolfers and Zitzewitz, 2016; Hwang and Rosen, 2017; Ohlin, 2017). Terms such as "post-truth," "post-fact" and "fake news" have sprawled in the academic landscape, serving as umbrella concepts to explain belief formation in an age where lies and rumor can spread through channels constructed as "reliable sources of knowledge" (Vargo *et al.*, 2017; Watts and Rothschild, 2017; Boyd-Barrett, 2018; Guo and Vargo, 2018; Tandoc *et al.*, 2018; Braun and Eklund, 2019). Works addressing these notions have been critical to raising awareness of the central role that digital-media-propelled discourse, knowledge and reality perception have come to play in the conditioning of individuals' political views and behaviors. However, most of them implicitly take as a point of departure the idea that "the nightmare scenario" that they ultimately try to explain—the election of Donald Trump— was first and foremost caused by the sharing of "misinformation" about Hillary Clinton. Frequently, this line of reasoning has led to conclusions that suggest that equal or similar abysses can be avoided with the help of "responsible journalism," "responsible politicians" and the commitment from Internet socialization and search platforms to somehow prevent the spread of "false" information (Corner, 2017; Tambini, 2017; Haigh, 2018; Lazer *et al.*, 2018; Waisbord, 2018). This prescription introduces the flawed assumption that the danger lies in the quality of the information being published and shared as "facts."

What seems to have gone mostly unnoticed—or not taken seriously enough—is the structural power of the cyber-spatial mechanisms through which "fact" is constructed as "fact" and "truth" is constructed as "truth." Regarding the American presidential election of 2016, such observation could have led analysts to ask, to what kind of *dispositif* (Foucault, 1980, p. 138) does the U.S. attribute the power of managing

---

point in history in which four geopolitical conditions coincide: besides being deemed an attack against the U.S., motivating a formal declaration of state of emergency, triggering economic, diplomatic and cyber retaliatory actions against the alleged attacker, it was solely conducted over cyberspace. Other countries have been subjected to similar types of operations, sometimes through more rudimentary means of discursive construction, and sometimes through essentially the same as the ones that were used to meddle in the American election. Yet I was unable to find any information on subsequent retaliatory actions taken by the injured parties.

people's perceptions of their environment to the extent that an injection of information contrary to its elites' interests can be easily constructed as an attack on its sovereignty and be tacitly acknowledged as the cause of irreparable damage to its immediate agenda? This dissertation is an exploratory study and a conceptual exercise with the goal of providing the first brushstrokes for the analysis of such *dispositif*; a constellation of phenomena, hitherto spoken about and studied as discrete events and functions evolving in cyberspace, but with no cohesive theory explaining their interplay in connection to sociopolitical actors and processes.

This phenomenon is characterized by partially observable dynamics; a fundamental reliance on unstructured and semi-structured, semantically rich, user-generated data; the machine-assisted construction of political narratives designed for the instrumentalization of national agents; and the steering of their communicative actions towards the precipitation of a rupture with the normal sociopolitical order. Therefore, this phenomenon can be provoked and orchestrated to bring about an instrumental rupture with normalcy. In the case of the American presidential election of 2016, this rupture was leveraged in the building and destruction of candidates' legitimacy. However, as the Obama administration showed the world, the same event constructs utilized in the rupture can be repurposed and reused in other strategic political narratives (Obama, 2016b; a; United States, 2016c).

For instance, when questioned about the revelations emerging from the Democratic Party's leaked emails, the Clinton campaign responded by alleging that the emails had been hacked by parties working for Russian State actors in purported collusion with the Trump campaign (Chozick, 2016; Mook, 2016). Months later, the official intelligence report on which then-President Obama based both the economic and diplomatic sanctions against Russia and his state of emergency decree of December 29, 2016 contained little more than the information that the Clinton campaign had already made public via statements on mainstream media back in June of the same year (Office of the Director of National Intelligence, 2017). Therefore, the same narrative elements used to try to destroy Trump's legitimacy as a candidate and potential president were later used to legitimize an act of aggression against Russia. And though the latter turn of events set a precedent for a type of scenario that requires the attention of the field of international studies, it is only by studying the underlying phenomenon that such scenario can be stripped away of its semblance of objectivity and be rendered falsifiable.

Analyzing the underlying phenomenon instead of taking “the act of foreign interference” as a point of departure also opens the possibility of observing other potential paths along which the *problematique* may evolve. Thus, while approaching the phenomenon as detached from the fate of the narrative of foreign aggression it is possible to observe Donald Trump’s own disruptive mass movement as an instrument for the infliction and enlargement of a rupture with normalcy that, according to his narrative, only his construct of himself—the savior strongman—was capable of governing. This is in part because the process entailed a quasi-Biblical feat: “pulling the country out of the hell” that his opponent’s party had led it into (Wojnowski, 2016). Thereafter, the dramatization of Trump’s disruptive narrative indeed made the rupture illustrate “the hell the country had turned into.” How could Clinton “be the one to deliver Americans from evil” if it was her own party that “had left the country in shambles”? By association, she became unfit to be president. Complementary to this was the “crooked Hillary” narrative. The emblematic Establishment politician, selling political favors in exchange for donations to her foundation, using part of the proceeds to fund the political causes of her allies in the party, the same who helped her undermine Bernie Sanders and “steal” the primaries from him (Bond *et al.*, 2017; McHale, 2017). Both the narrative of the “unethical politician” and the narrative of “complicity with the makers of the status quo” reinforced each other. I would argue that the dramatization of this discursive dynamic in both the virtual and physical dimensions of the public sphere sealed her demise as a candidate.

However, just as the phenomenon underlying the construction of these political narratives is independent from the eventual denomination of its manifestations as instances of “foreign interference” or “foreign aggression,” it is also not circumscribed to electoral periods or party politics. Its mechanisms and propellant forces had been at work well before the 2016 American presidential campaign period and they continue to be, for they are powered by the algorithms that handle the construction of “knowledge” in the informational society. Hence, the study of the inter-party discursive power struggle for the construction and destruction of presidentiable characters is not the primary objective of this conceptual exercise.

Rather, the value in analyzing the phenomenon against the backdrop of the American presidential election of 2016 lies in the light it shed on the phenomenon’s structural components, which are usually characterized by the fuzziness and opaqueness of their interrelationships. In mise-en-scène: political-party actors; State

actors; private sector actors; intersubjective discursive construction processes regulated by deep-learning, virtual robots; content prosumers mined for their data, weaponized to produce instrumental environmental conditions through the manipulation of their "knowledge;" for a few months, a few black boxes turned semi-transparent.

In the final analysis, the American presidential election of 2016 portrays the kind of power that political figures can have access to when they have the resources to "rent" the virtual communication machinery capable of defining and engaging audiences in the terms necessary to inflict the socio-systemic crises that they need for the legitimation of their authority. Neatly outlined on the foreground stand out the specific knowledge-construction mechanisms capable of evocating the emotions that ignite volatile sociopolitical environments. Their identification is part of the benefits of focusing on the underlying phenomenon as well, for their isolation makes it possible to analyze of changes in patterns of sociopolitical behavior as a function of cyber-spatial discourse construction.

1.2. CAVEATS

I offer two, most-warranted caveats from the outset. First, although this work is intended to serve as a theoretical incursion into the point of convergence among the automated mechanisms for the construction of political narratives on cyberspace, the building and erosion of legitimacy, and the creation of ruptures in systems' political order, this dissertation can only hope to lay the groundwork for a theory; it falls short from being one. Second, there are methodologies and methods that need to be integrated for the measurement of the proposed phenomenon's processual components; they exist but such integration is beyond the scope of this dissertation. The latter caveat is one of the main reasons why I would not consider the work to be ready for a review that could evaluate its validity as a full-fledge theory. Coupled with the fact that the conditions for "an attack on a country's sovereignty" similar to the one that Washington denounced in late 2016 are latent, the second caveat is also the reason why I would recommend that the field of international studies finds the resources necessary to remedy such shortcoming as soon as possible. Even if such analytical capability will do little to avert future scenarios of "digital marketing

interference," it will at least enable the field to take aim at the inherently discursive nature of the events and actions being denominated "international aggressions." This could then serve as a leverage point to question the justifiability of entering conflict in any capacity. This leads me to two more points of clarification.

This dissertation does not conceptualize the phenomenon under study as a type of "act of war," "foreign interference" or "foreign aggression" per se. The act of framing the phenomenon as such is itself a manifestation of the phenomenon, and the denominations are part of its repertoire of discursive products. Accordingly, this dissertation does not concern itself with the question of whether external propagandistic support or undermining of a country's political candidates should be considered "sufficient grounds" for retaliatory action on the part of the allegedly injured party. Along the same lines, contributing to the ongoing debate on the construction of a framework outlining the liberties and limitations that countries should embrace to materialize international coexistence on cyberspace is not one of this dissertation's intended goals. Although the case study referenced herein could serve such purpose by questioning the conditions under which the publishing of multimedia content on privately-owned socialization platforms governed by the logic of "free speech" could justify or legitimatize entering an escalating spiral of mutual aggressions between two States.

1.3. THE BIRTH OF A CONCEPT

In the most specific of terms, the phenomenon I sought to explain could be described as the sum of the machine-learning instruments used in, and the discursive and behavioral sociopolitical outcome of a top-down, concerted, yet mostly automated communicational effort to build or erode legitimacy for a political agent or action, leveraging the systematic manipulation of individuals' emotions through cognitive-semantic experiences. Searching for parallels in the existing literature, I found most of my definition's essential elements represented in John Arquilla's and David Ronfeldt's formulation of the information warfare doctrine, developed under the auspices of the RAND Corporation. Phrased as an adaptation of Carl von Clausewitz's definition of "war" (Clausewitz, 2007, p. 13) to the Information Age, Arquilla and Ronfeldt understand information warfare as "the use of information to impose one's will upon an

adversary—often via cyberspace, but more often by traditional means (e.g., public diplomacy, propaganda, psychological operations, and perception management) (Arquilla and Ronfeldt, 1997b, p. 14).” The similarities between this framework and the definition that I devised provided a promising start in the quest for a pre-existing working concept due to more than just their degree of mutual compatibility. On the one hand, the Pentagon’s incorporation of the information warfare doctrine into its Revolution in Military Affairs (RMA) framework confirmed—though indirectly—the pragmatic, political and historical relevance of my conceptualization—it also provided a rationale for the framing of the “anti-Clinton” campaign as an attack on the U.S. On the other hand, locating my conceptualization of the phenomenon under discussion within the theoretical grounds of Arquilla’s and Ronfeldt’s work placed it within a body of scientific contributions whose systematic formulation of the information warfare framework is considered seminal to issue experts and strategists alike. This is due in part to a key taxonomical characteristic that expands its congruence possibilities, making it applicable to both military- and societal-level engagements, which they identify as “cyberwars” and “netwars,” respectively.

Thus, oriented by Clausewitz’s maxim that “knowledge must become capability” (Clausewitz, 2007, p. 97), the “cyberwar” modality of information warfare seeks to create the material conditions where “the balance of information and knowledge” is turned in favor of the party waging war. It does this by:

> Conducting, and preparing to conduct, military operations according to information-related principles (…) disrupting if not destroying the information and communications systems (…) on which an adversary relies in order to “know” itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first (…) trying to know all about an adversary while keeping it from knowing much about oneself (Arquilla and Ronfeldt, 1997a, p. 30).

My conceptualization can relate to Arquilla’s and Ronfeldt’s “cyberwar” in the instrumental role given to “knowledge” and “information” in the process of subjugating a third party by controlling access to the means of knowledge construction. However, their notion appears to be anchored in the idea of executing a series of coordinated belligerent actions. Cyberwar “adversaries” have motivations as lethal as they would if they were waging any other kind of warfare. They seek to annihilate the other, what changes is the central role that “knowledge” and “information” play in the process. While my conceptualization does not exclude the possibility of military engagements to ensue as a result of the phenomenon’s development, the realization of such scenario

is neither necessary, nor sufficient for it to acquire the conditions that I consider distinctive in its approach to building or undermining a political agent's or action's legitimacy. In this sense, Arquilla's and Ronfeldt's "netwar" notion specifies actors, objectives and methods that suggest greater compatibility with my conceptualization of the phenomenon:

> Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote a dissident or opposition movements across computer networks. Thus designing a strategy for netwar may mean grouping together from a new perspective a number of measures that have been used before but were viewed separately (Arquilla and Ronfeldt, 1997a, p. 28).

While "cyberwar" describes a traditional scenario of lethal engagements with new instruments to "blind" the adversary while destroying its material means to construct knowledge and information, "netwar" takes "war" outside the traditional battlefield context, bringing it to the realm of ideation. Targets are no longer infrastructural components in telecommunications networks; they are audiences. The "destruction" of both adversaries and the means of information and knowledge articulation is superseded by their reprogramming as producers of instrumental "knowledge" and "information," tailored to serve a grand strategy's objectives. Nevertheless, Arquilla and Ronfeldt stopped short of stating explicitly a key conclusion stemming from their argumentation: "knowledge becomes capability" when interference in audiences' belief-construction processes permits their behavioral conditioning and domination. Although it is somehow suggested in the mentioning of methods such as "propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media," the link between netwars' information and knowledge utilization mechanisms and war scenario types remained missing. As a result, it is unclear what role the authors envisioned for the target audiences in the context of netwars "between the governments of rival nation-states, (…) governments and non-state actors" (Arquilla and Ronfeldt, 1997a, p. 29) and "between rival non-state actors" (Arquilla and Ronfeldt, 1997a, p. 30). As far as my conceptualization is concerned, this was a salient shortcoming for it steered the argumentation away from the point that brought the "netwar" concept the closest to it. It is a tacit conclusion that follows from the aforementioned: the disruption of audiences'

belief-construction processes is carried out with the intention of "weaponizing" individuals, creating the psychological conditions for them to manifest behaviors that may be instrumental to a grand strategy's objectives. Could developing this sequence of conclusions have made the "netwar between rival non-state actors" scenario apt to evaluate the American presidential election of 2016?

In his book, "Cyber war will not take place," Thomas Rid points out:

> "War is an act of force to compel the enemy to do our will," wrote Clausewitz (…) If an act is not potentially violent, it's not an act of war and it's not an armed attack—in this context the use of the word will acquire a metaphorical dimension (…) A real act of war or an armed attack is always potentially or actually lethal, at least for some participants on at least one side (…) The same applies to the idea of a weapon. In Clausewitz's thinking, violence is the pivotal point of all war (Rid, 2013, p. 1-2).

Others such as Brandon Valeriano and Ryan C. Maness (Valeriano and Maness, 2018) and Erik Gartzke (Gartzke, 2013) have voiced similar opinions. "War without violence and death is not a war" (Valeriano and Maness, 2018, p. 5); a criticism that can be evidently applied to the concept of "netwar" as well. Moreover, even if all kinds of information warfare were to be unanimously accepted as types of "war," neither the American presidential election of 2016 could be defined as an instance of "war," nor is the instrumentation of violence a sine qua non condition for the phenomenon that I conceptualized. Yet, at the same time, the striking similarities that my conceptualization bore to the netwar modality of information warfare could not be overlooked.

Taken together, the aforementioned shortcomings, discrepancies and similarities delineated a three-point path to the concept I was looking for: it would be included in the realm of netwar-related literature, it would not be categorized as a type of "war" and it would refer to one or more processual instruments for the domination of audiences' belief-construction systems with the goal of conditioning their sociopolitical behavior. Further, meeting two more requirements would make it an ideal working concept: having the building or erosion of agent or action legitimacy as its instrumental goal and relying on deep-learning machines for the systematic manipulation of individuals' emotions through the construction of cognitive-semantic experiences.

Thomas Kuhn would have probably pointed out that the first factor to bear in mind for the next stage of my conceptual quest was the scientific paradigm in which Arquilla and Ronfeldt produced their information warfare (Kuhn, 1996). In 1993, machine-learning technologies were just about to start their rise to the center stage of

the world's predominant realm of knowledge construction. The mechanisms that would grasp user web activity and turn it into shareable data for machine-learning, communicational systems would not become widely used until the late 2000s. Therefore, since the production of scientific ideas is influenced by technology as much as technological innovation is an expression of scientific revolutions, the search for a concept capable of describing a phenomenon with the characteristics that I formulated would be fruitless, unless I adjusted my timeframe, or opened myself to the possibility of not finding an exact match.

I decided to fast-forward in time and resume my search from a scientific context with a direct ontological, epistemological, methodological connection to the one in which Arquilla and Ronfeldt designed the information warfare framework: the RAND Corporation and its graduate school.[3] Some of the most influential ideas to come out of this context were delivered by RAND's Deputy Chief Technology Officer and former professor Rand Waltzman, in the form of a testimony before the U.S. Senate Committee on Armed Services on April 27, 2017. The occasion would mark a point in which the phenomenon referenced itself through one of its products; a hearing on "Cyber-enabled Information Operations" to assess the threat posed by Russia and other foreign powers with cyber offensive capabilities. Waltzman's testimony would also be the first time that high-ranking members of the American national security apparatus were presented with an expert's account that described the phenomenon as a single entity integrating a constellation of cyberspace communicational processes:

> Today, thanks to the Internet and social media, the manipulation of our perception of the world is taking place on previously unimaginable scales of time, space and intentionality. That, precisely, is the source of one of the greatest vulnerabilities we as individuals and as a society must learn to deal with. Today, many actors are exploiting these vulnerabilities. The situation is complicated by the increasingly rapid evolution of technology for producing and disseminating information (…)
>
> Traditionally, "information operations and warfare, also known as influence operations, include the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent." This definition is applicable in military as well as civilian contexts. Traditional techniques (e.g. print media, radio, movies, and television) have been extended to the cyber domain through the creation of the Internet and social media.
>
> These technologies have resulted in a qualitatively new landscape of influence operations, persuasion, and, more generally, mass manipulation. The ability to influence is now effectively "democratized," since any individual or group

[3] The Frederick S. Pardee RAND Graduate School, which offers a multidisciplinary, policy analysis Ph.D. program.

> can communicate and influence large numbers of others online. Second, this landscape is now significantly more quantifiable. Data can be used to measure the response of individuals as well as crowds to influence efforts. Finally, influence is also far more concealable. Users may be influenced by information provided to them by anonymous strangers, or even by the design of an interface. In general, the Internet and social media provide new ways of constructing realities for actors, audiences, and media. It fundamentally challenges the traditional news media's function as gatekeepers and agenda-setters (Waltzman, 2017, p. 1-2).

Clearly, Waltzman's testimony was coherent with the logic of "waging war" through ideation present in Arquilla's and Ronfeldt's "netwar" concept, recalling its core process of exploiting individuals' perceptions of the world through the mediatic construction of "realities" to the advantage of a mastermind orchestrator. However, Waltzman also introduced new elements that made his account of the current conjuncture much more approximate to my conceptualization of the phenomenon of interest. In the landscape that Waltzman projected, leaving behind the sole function of literal calculations, data rises to the role of describing and communicating steps in interaction sequences, which together express "states" in behavioral trends. Thus, data now has a critical function in the successful manipulation of individuals, for it is how their feedback is communicated and measured for strategic response. "User experience narratives" result from these sequences of calculated responses, architected to further influence specific user interactions with information.

By now, people have been successfully indoctrinated to confer power to repetitive graphical patterns; symbols which they have been taught to assimilate as "representatives" of other people or system functions. These symbolic patterns have functionalities that, if they happen to break with "digital-world" standards, their intuitive designs, repetitive inputs and outputs and routinary functions within overarching workflows make them prone to learnability. Their ease of usage leads to their osmotic adoption, and their simplification of complexity encourages their incorporation into all dimensions of daily life. Hence, social activity develops dependencies on their continuous performance of assigned tasks for their outputs are expected as inputs elsewhere (e.g., a function in a Google Spreadsheet expects a result from another in order to generate an output used in yet another; Peter expects the result of the chain of functions, so his boss can get his report out the door; John awaits Jane to finish typing a response to his question, "so, is it a date?" He has spent one and a half minutes looking at three little dots that are supposed to indicate that she is still typing her answer somewhere in the world). These expectations imply trust in the user

experience narratives that communicate the expected functional performances. Behind these instances of trust there is the power of influence and potential for concealed manipulation.

Furthermore, through the mention of “propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media” as methods to disrupt a “target population’s” knowledge of itself, Arquilla’s and Ronfeldt’s seem to make allusion to the “target audience” construct, a classic component of “psychological operations.” However, as netwars are ontologically attached to military conflict, so are psychological operations—at least such is the implication of Arquilla’s and Ronfeldt’s logic. According to Carnes Lord, this logical conclusion would also coincide with the operations’ actual tendencies in the U.S. military which, “historically, (…) [its] interest in [psychological operations] has focused heavily on tactical applications in wartime” (Lord, 1989, p. 19). In theory, however, psychological operations do not need to be undertaken only in a context of military conflict, just as “adversaries” do not have to be considered their only possible targets. In fact, to consider psychological operations a type of “warfare” is altogether problematic in practical terms (Lord, 1989, p. 17) and Waltzman highlighted one of the main reasons for this in his testimony. He explained that “while the Westerners see IO [information operations] as limited, tactical activity only appropriate during hostilities (…)[,] for the Russians IO are a continuous activity, regardless of the state of relations with any government[.] In other words, Russia considers itself in a perpetual state of information warfare, while the West does not” (Waltzman, 2017, p. 4). And, since ICTs enable “any individual or group [to] communicate and influence large numbers of others online,” the psychological operations’ target audiences make the threat be perpetual without even realizing it.

This is why, to Waltzman, the way to counter the Russian threat is through a nationwide information defense strategy framework; “a coordinated effort between national government organizations, military, intelligence community, industry, media, research organizations, academia and citizen organized groups” (Waltzman, 2017, p. 5) But what his vision entailed was the employment of the same technologies that Russians would use in a psychological operation attack in a series of countermeasures oriented to shielding Americans from the effects of Russian tactics (Waltzman, 2017, p. 6-7). This explains why Waltzman had to make an explicit distinction between both “warfare” and “operations,” and “military” and “civilian” contexts, for defending the

population from a psychological operation would entail preparing a psychological operation of their own. For instance, consider this fragment from ex-Secretary of Defense Donald Rumsfeld's "Information Operations Roadmap" report:

> Considerable effort should be made to characterize potential adversary audiences, and particularly senior decision-makers and decision-making processes and priorities. If such human factors analysis is not conducted well in advance of the conflict, it will not be possible to craft PSYOP themes and messages that will be effective in modifying adversary behavior (Rumsfeld, 2003, p. 21).

To counter this type of move, the country's authorities would have to map potential "target audiences," their key influencers and sociopolitical dynamics and speculate on the types of messages that could be most effective in modifying their behavior. Once this surveillance and microtargeting calibration process is completed, a domestic psychological operation to prevent the modification of behavior would take place. If the U.S. were to conduct the same actions using foreign audiences as targets, then the "psychological operation" could be framed as an act of "warfare." In Waltzman's framework, these actions would be legitimized as acts of national security carried out to guard against Russian psychological operations. Accordingly, he baptized his solution as "cognitive security" (Waltzman, 2017, p. 7).

> The massive explosion of behavioral data made available by the advent of social media has empowered researchers to make significant advances in our understanding of the dynamics of large groups online. However, as this field of research expands, opportunities multiply to use this understanding to forge powerful new techniques to shape the behavior and beliefs of people globally. These techniques can be tested and refined through the data-rich online spaces of platforms like Twitter, Facebook and, looking to the social multimedia future, Snapchat.
>
> Cognitive security (COGSEC) is a new field that focuses on this evolving frontier, suggesting that in the future, researchers, governments, social platforms, and private actors will be engaged in a continual arms race to influence—and protect from influence—large groups of users online (Waltzman, 2017, p. 7).

Thus, Waltzman's "solution"—which is the most unique piece of his entire contribution— encapsulated the most salient characteristics of the phenomenon that I had initially conceptualized. Yet, he framed it as a "solution," when in fact the "arms race to influence—and protect from influence—large groups of users online" is one of the processual components of the phenomenon as it is today—there is no need to wait, "the future" is here. The social platforms that he mentioned—as well as all major search platforms—already "influence and protect from influence." These "machine-learning instruments used in the systematic manipulation of individuals' emotions" do so by

structurating their “cognitive-semantic experiences” through algorithms that regulate “what” pieces of “knowledge” get to “define” what they search for. Then, they arrange the graphical elements that construct users’ online experiences in such way that the compositions are always “relevant” vis-à-vis these definitions. I do not see Waltzman’s “cognitive security” as a solution; considering his testimony’s topic, his audience and the venue, I see it as petition to legitimate a State-sponsored, domestic, psychological operation. It will most likely be “top-down, concerted, yet mostly automated,” but it is not clear to me whether it will be used “to build or erode legitimacy for a political agent or action.” Out of all of my conceptualization’s critical points, the instrument’s end is what Waltzman’s “solution” seems to be missing.

Even with these shortcomings, Waltzman’s incorporation of the “cognitive” dimension as part of “the problem to be solved” confirms that, even if addressed as a “military vulnerability,” the issue needs to be understood as a phenomenon that is not inherently political-military. Waltzman concludes his testimony by making a formal requisition for resources to fund what would be the start of his “whole-of-nation” “cognitive security” program:

> What is needed is a Center for Cognitive Security to create and apply the tools needed to discover and maintain fundamental models of our ever-changing information environment and to defend us in that environment both as individuals and collectively. The center will bring together experts working in areas such as cognitive science, computer science, engineering, social science, security, marketing, political campaigning, public policy, and psychology to develop a theoretical as well as an applied engineering methodology for managing the full spectrum of information environment security issues.
>
> The center should be nonprofit and housed in a nonprofit, nongovernmental organization that has international credibility and close ties with government, industry, academia, think tanks, and public interest groups internationally (Waltzman, 2017, p. 7).

Waltzman’s “cognitive” approach was absolutely relevant, for it is precisely the mind’s psycho-cognitive processes that affect human behavior. After a concise, not exhaustive, review of the literature on the field’s basic definitions, I concluded that the processes of attention, working memory, procedural memory, semantic memory, episodic memory, perception and language are most connected to the phenomenon of interest. However, while acknowledging the importance of understanding these processes’ mechanics to form a complete and accurate comprehension of the phenomenon’s micro dynamics, an analysis at such level was out of the scope of this research project.

After analyzing all information surveyed, I concluded that the literature did not yet have a proper concept to describe the phenomenon that I sought to study. However, following the RAND Corporation's work on information warfare from its inceptions I was able to find enough indicators to make an informed decision as to the name with which I will be referring to the phenomenon henceforth. Thus, I integrated the words "cyberspace," "psychological," "cognitive" and "operation": cyber-psycho-cognitive operation. Perhaps time will provide a shorter, more suitable name, but this one seems logical and usable for the task at hand.

1.4. METHODS, THEORIES AND ARGUMENTS

In the previous section, I began the formulation of the "cyber-psycho-cognitive operation" concept utilizing elements of the Foucauldian-Nietzschean genealogical method for the study of history (Foucault, 1977). This seemed to me the most adequate method to give birth to a conceptual product of the discursive discontinuity characterizing the scientific framework that communicates both the observations and prescriptions of one of the most influential think tanks vis-à-vis the American security apparatus. "What is found at the historical beginning of things is not the inviolable identity of their origin; it is the dissension of other things. It is disparity" (Foucault, 1977, p. 142). This discontinuity was evidenced not just across scientific paradigms—before and after the 2016 presidential election; before and after the rise of social platforms with artificial intelligence. There are theoretical discontinuities in past and present: "information warfare," "psychological warfare," "psychological operations," "political warfare," "information operations," "ideological warfare" or "the war of ideas" do not "mean" the same but they are used to designate similar activities because "this sort of warfare is waged to a considerable extent with weapons that are not truly distinctive" (Lord, 1989, p. 16).

The theoretical discontinuities are not just inconsequential "expressions." Their discursive contexts produce transcendental practical implications, from how the phenomenon is approached, to how it is to be dealt with—if at all—and "the parameters of practice." Comparing and contrasting Arquilla's and Ronfeldt's information warfare framework with Lord's views on "The psychological dimension in national strategy" and Waltzman's testimony to the U.S. Senate Armed Services Committee, it became clear

that the American security apparatus struggles with such issues as separating “operation” from “warfare;” deciding whether “warfare” can be applied during “peacetime” to “friendlies” and “civilians,” or if it is it just reserved for “wartime” and “adversaries;” or if the nature of the “practice” changes qualitatively with the jurisdiction in which the “target audience is located.” When confronted with the task of developing a concept that can both acknowledge and represent these contradictions, the most sensible approach is to expose "not a timeless and essential secret, but the secret that they have no essence or that their essence was fabricated in a piecemeal fashion from alien forms” (Foucault, 1977, p. 142). And I followed suit, I fabricated my concept with the scraps that the scholars and practitioners left behind. The Foucauldian-Nietzschean genealogical method “opposes itself to the search for ‘origins’” (Foucault, 1977, p. 140) because a historical study that departs from such assumption is bound to a logic prone to ignore the elements of uncertainty and probability that underlie the collision of agents, places, events and scenarios.

It was one such kind of moment that provided me with the last “semantic pieces” that I needed for my concept; a critical point in the trajectory of the phenomenon. I am talking about the “historical accident” where the Deputy Chief Technology Officer of one of the most influential thinktanks in the American security apparatus addresses the U.S. Senate Armed Services Committee about “a permanent Russian information operation”—the existence of which is possible, but its verified factuality only goes as far as the utterances in his narrative. On the day of Waltzman’s testimony collided the once abandoned (Lord, 1989, p. 13), yet later resumed consideration for “some form of” information-psychological operation targeting the civilian population at home (Hawkins, 2003, p. I-4; Rumsfeld, 2003, p. 74); the rich, yet fuzzy conceptual baggage dragged since before the rise of the information warfare framework and the testimony’s most relevant political functions for the context of April 27, 2017.

Waltzman’s performance was an act intended to provide the basis for legitimacy for the implementation of a “whole-of-nation cognitive security strategy” that had presumably not started yet. This testimony’s symbolic function was based on pure fiction, for the program’s alleged novelties—in short, a triple-helix partnership for the development and deployment of automated communicational systems to micro-target audiences with strategic information—have been gradually built and turned operational over the course of the past seven decades. RAND knows this; it has been there every step of the way. However, the testimony’s factual function—the one that it served upon

delivery—was to provide further support for one of the cyber-psycho-cognitive operations that made its debut in American mainstream media during the presidential campaign of 2016. A story about a political candidate who was being helped by the Russians by attacking his rival.

The economic, political and cultural *dispositif* that Waltzman sold as a novelty is the same one that "turned knowledge into capability" in favor of the detractors of Donald Trump in the lead-up to the election and beyond. "Warfare" or not; "military" or not; the practices, the platforms, the algorithms, the pool of "target audiences" and the nonvirtual actors are all the same. What changes are the messages, the end goals and the "sales pitch." The following chapter in this dissertation, "The accidented road to the current paradigm: Economy-driven proliferation of ICTs' users and uses," is a historical exploration into the scenarios of convergence between and among inventors, materials, interfaces, political and military projects, cultural, economic, communicational trends and other contingencies that formed and continue to propel this *dispositif*.

Given that it had been deemed a "security" threat, more than just a curiosity to know the phenomenon's trajectory, what guided this chronological overview was a need to identify the conditions of possibility for its neutralization. To this end, I first pondered a series of basic premises. First, at the heart of any cyber-psycho-cognitive operation lies the dissemination of ICT-driven narratives capable of building and eroding political authority. Second, as both the construction of political narratives and their linkage to the formation of legitimacy predates the ICT revolution, the critical independent variable to the successful execution of a cyber-psycho-cognitive operation seemed to lie in ICT devices' operational properties and their relationship to narrative composition, sharing and consumption. More specifically, the use of ICTs' functionalities appears to have led to the development of intersubjective discursive construction modalities that incite agents not only to engage in the creation, propagation and intake of narratives, but also in the near-uncontested and instantaneous formation of beliefs with a bias towards regarding their claims as "facts." Third, the formats in which these narratives are presented and experienced, as well as the wide variety of opportunities for interactivity afforded by the platforms in which they are embedded invite agents to articulate types of intersubjective dynamics that tend to be as immersive as they are emotive. Fourth, these emotion-arousing experiences

seem to turn narratives into triggers for increasing political engagement, not just in the private, but also in the public sphere.

Considering the above, I initially cogitated approaching the historical overview as a task to shed light on the material or immaterial conditions without which ICT-driven political narratives would cease to evoke the type of belief-construction and emotion-arousal scenarios that could be decisive in the building or erosion of legitimacy. Though highly relevant to the development of a deep understanding of the cyber-psycho-cognitive operations, it seemed as if the fruit of such historical inquiry was bound to have limited utility beyond the overview itself, for I was not going to be able to submit the findings to a validation test. In short, the quest seemed unfeasible because the financial, technological, technical and knowledge resources available were insufficient to carry out a qualitative research designed to account for two facts that were key according to the inquiry's specific articulation. On the one hand, though they are prone to collective influence, the psycho-cognitive processes that relate to belief-construction and emotion-arousal are experienced individually. In the context of ICT-based communication, they are the result of a relationship between a message receiver and the material and immaterial round-trip message conveyance mechanisms mediating the communication experience. On the other hand, the aforementioned mechanisms are produced and accessed in mass.

A qualitative research capable of accounting for these two factors would have to employ one or more methods to gather data from one or more prolonged, real-life scenarios, fostering spontaneous responses, involving massive numbers of ICT users interacting over a platform capable of capturing users' clicking, mouse-hovering, eye movements and, of course, all of their data creations (i.e., searches, URLs shared, words typed, posts, videos watched, etc.). The platform would also store these events as data for later aggregation and enrichment, associating them with the time, location, device and demographic parameters describing their occurrence. Moreover, content would have to be categorized and annotated according to a previously-crafted glossary containing the value associations between emotions and semantic expressions. Once these data setups were completed, the analyst could obtain reports relating the aforementioned variables and henceforth derive conclusions. Nevertheless, as this experiment was beyond scope, the historical overview had to pursue the identification of the conditions for the "security threat's" potential neutralization using an approach

that could produce valid and plausible answers without the need to rely on hard empirical data.

The solution that I came up with was a reformulation of the analytical inquiry that could permit the application of a rational test grounded on historical facts: how have the economic factors leading to the social penetration and expansion of ICTs influenced the formation of a practice of narrative belief-construction? There are two underlying assumptions in this new formulation. First, that the evaluation of factuality of a piece of information precedes its effect in the individual's emotions; the all-too-frequent case in which the individual appears to forego the evaluation is simply an expression of "presumed factuality." Second, that inflicting changes in the aforementioned economic factors could perhaps suppress the practice of belief-construction on which the effectiveness of cyber-psycho-cognitive operations rests. Having reached an adequate logical grounding, the reformulated inquiry led the historical overview through an analysis of the material peculiarities that contributed to the formation of an innovation cycle acceleration based on inverse relationships between, on the one hand, exponential increases in computing output and, on the other, decreases in both data processor sizes and their market prices. As more computing power furthered innovation acceleration, every cycle kept turning out ever smaller, yet more powerful and cheaper processors. The resulting self-recursive spiral would eventually create all the necessary material conditions for a potential adoption of computers in all dimensions of social activity. Yet, this society-wide adoption would have never been possible had there not been groundbreaking design innovations that permitted people to access advanced data processing capabilities regardless of their prior computer programming knowledge. This entailed the configuration and intensive use of increasingly simple sequences of symbolic input actions to command predictable outputs resulting from increasingly complex computations.

Thus, "user interfaces" were born; physical and virtual object arrangements invoking the performance of user input actions through intuitive hints designed to trigger the execution of machine functions that have been preprogrammed to repeatedly produce predictable results. They are organized to serve specific interaction purposes; therefore, when they are not altogether connected to one another programmatically, they are still designed to appear as if they relate to one another conceptually. At the level of user-information experience, they manifest as interactive narratives. They are perceived as object types conveying a connection to one or more

desirable outcomes. Users are led to believe that these outcomes are the direct or indirect effect of the performance of the particular kinds of input actions that the routinary narratives incite them to complete. As the performance of the same input action over the same interface object produces the same results every time, their behaviors become predictable. To the point where users get to think that they can safely assume that carrying out the same input actions over the same object types anywhere on the web will always produce the same type of results. As the standard application of programming design patterns across the web has ensured that most of the time they do, the constant dramatization of the behaviors resulting from the utilization of this functional assumption appears to have engendered a kind of state of mind where the performance of such actions can be executed in an automatized fashion. Embedded in contexts constructed with these user interfaces, content that should be subjected to critical thinking is consumed under a type of state of mind that is akin to automatized information interaction. Hence, users seem to carry over to the realm of content consumption the trust implicit in the assumption that user interface functionalities can be relied on to produce the same results all the time. This is directly related to the belief-construction phenomenon that lies at the heart of cyber-psycho-cognitive operations.

Although user interfaces were not born as the advanced interactive mechanisms they are today, their rudimentary emergent state provided enough to begin the process of “popularizing” microcomputers. All conditions came into alignment for both a relentless socioeconomic and geographical penetration of ICT use and their functional expansion in everyday life. Increasingly faster innovation cycles meant faster turnover of increasingly advanced devices. Steadily decreasing prices meant that even people with restrained purchasing power would eventually be able to own devices with advanced capabilities. Smaller, yet more power processing units incentivized innovators to embed nano data processors into artefacts that were either altogether new or had never been computerized. Newly-computerized artefacts and accessories kept their old names but got their functions redesigned according to a data-generation-and-sharing logic, powering a whole new layer of ubiquitous computing. Suddenly, activities performed in both the public and the private spheres, no matter how intimate, could generate contextually-rich data. Once aggregated with the data produced by all the other devices, artefacts and accessories, these data could serve to develop a profile based on the person producing it. In essence, this is how life has become

datafied. And insofar as interacting with data objects is both intuitive and indispensable to be and remain “relevant” in the informationalist mode of development, people’s livelihood will, to a large extent, depend on their interaction with narratives (Castells, 2010b). This, however, is far from being a “painful” process. The web has learned from social media platforms the art of gamified design, thereby making user-information experiences more engaging and immersive. Consuming content is presented as a “free” and seamless experience, yet this seemingly passive activity generates the metadata that is transmitted and sold as raw material for data mining; eventually it is used as input to target advertising campaigns. The contextual specificity inherent to ICT devices’ ubiquity adds an invaluable layer of information to further enrich this targeting mechanisms with a variety of data points. Thus, the second chapter reaches the conclusion that, far from existing any conditions whose undoing could foreseeably neutralize the emergence of cyber-psycho-cognitive operations, the material and immaterial economic factors driving the ICT revolution seem to make the execution of future operations highly likely. However, it is due to this apparent “inevitability” that developing a deeper understanding of their dynamics becomes all the more urgent.

Articulating a potential structure for the design of the cyber-psycho-cognitive operation phenomenon as an object of study was precisely the challenge that the third chapter wrestled with. The obstacles emerge from the intricate relationships between and among the actors involved, the political and technological mechanisms used to achieve their goals and the virtual resources that propel the operation. Moreover, these complexities are permeated by various degrees of opacity, some of which emanate from a type of political reaction characterized by the creation of regimes of what Max Weber called, “administrative secrecy” (Weber, 1978). The instauration of these regimes leads to both a lack of independent, scientific knowledge and the abundance of its “substitute”: media-produced “knowledge”—claims told as “facts,” whose veracity is uncertain and can also be part of an operation’s arsenal of ideation instruments. To be true, however, administrative secrecy is not a common denominator either. Some of the actors involved opt for being partially open about certain aspects of their capabilities, goals and even the roles they are willing to play “as a service” in exchange for data, money or both. Others are not even in a position to enforce personal data ownership or exert full privacy control—let alone impose a “regime” analogous to “administrative secrecy.” Thus, the context for data collection was all but homogeneous among elements that participate in the phenomenon in equally salient capacities. This

lack of uniformity transferred onto the approach with which their analysis was finally elaborated in the dissertation.

Though delineating a hardly ideal research scenario, these epistemic obstacles did seem to be in accordance with what a theory in its incipient stages could have to face. Nevertheless, also as expected, the current paradigm offered the tools and conditions necessary to surmount the challenges, even if only to the point of building a steppingstone in what seems to be a long path towards a complete theory. At a macrolevel, following both the logic of Norman Fairclough's Critical Discourse Analysis (Fairclough, 1995) and Kenneth Burke's dramatism (Burke, 1969), I approach cyber-psycho-cognitive operations as dramas in which content prosumers, data acquirers and generators, mainstream media, political parties and the State are engaged in an asymmetric power struggle, manifested through discursive events that demonstrate their drive to control the production, distribution and consumption of political narratives designed to build and/or destroy legitimate authority at a psychological level. In "Legitimation Crisis," Jürgen Habermas traced the root of this institutional vulnerability to the ambiguous relationship between "legitimacy" and "truth" as observed and articulated by Weber in his concept of "rational authority" (Habermas, 1992).

Essentially, the "rational" dimension of authority is directly linked to the perception that allies and subordinates have of their leaders. Therefore, it is in the authorities' best interest to continue performing actions that reinforce this perception. This is how they can project the image associated with the role for whose interpretation they were imbued with legitimacy, to put it in the dramaturgic terms of Erving Goffman; another key contributor to my theoretical framework (Goffman, 1956). Nevertheless, as Habermas points out, this would seem to imply that "legitimacy" is not permanent once granted. Rather, it is contingent upon the nurturing of beliefs about the political authority—those that sustain the psychological state in which the audience accepts that a specific political figure is fit to dominate them. And beliefs have no inherent connection to "truth." They can refer to phenomena whose factuality and veracity can be directly verified empirically. But they can also be the result of mistake, misguidance, or the conscious products of an individual or collective adherence to unverifiable claims. If legitimacy were tied to beliefs that necessarily referred to facts, then political authorities would have to perform real acts to maintain the alignment between the character that they constructed to be legitimized by the audience of allies and subordinates. In turn, this would require them to either be true embodiments of that

which they projected, or at least “truly become their projections” in order to “rise to the occasion.” But since the emergence of the communicational technologies to create and mediatize representations of what would otherwise have to be directly experienced before it could be believed to be both “real” and worth sharing as “knowledge,” everyone’s projected self has become a mere “perceived representation;” it has ceased to “have,” now it just “appears.” In this dissertation, I refer to these “representations of self” as “avatars;” Guy Debord refers to the society of mere representation as “The society of spectacle” (Debord, 1992). In my theoretical framework, authorities have taken advantage of this media-induced, representational condition of society to build and maintain legitimacy by constructing avatars that satisfy the beliefs necessary for the audience to continue experiencing the psychological state in which “ratifying” their legitimacy is “rational.” By the same token, others have sought to use the same mediatic instruments to undermine their political opponents’ avatars. Both types of strategies seem to construct “worlds” in which these avatars are or fail to be “legitimizable,” this is because despite the fact that they are “spectacles” they still need to seem “believable;” after all, they are articulated to provoke belief-construction. In this dissertation, I refer to these “worlds” as “narratives.”

Thus, cyber-psycho-cognitive operations take place in a context of discursive battles between and among political actors seeking to gain or maintain authority by managing public perception. Yet, the means to fight these battles—in fact, even the means through which the battlefield becomes perceivable—are owned by the media corporations, which, as actors in a play, Burke would argue, they have motives. I based my understanding of these motives on Noam Chomsky’s and Edward S. Herman’s analytical framework for the study of the structural factors influencing the ideas that the American mass media presents to the public through the news. Their “propaganda model,” developed in their work, “Manufacturing consent: The political economy of the mass media” (Chomsky and Herman, 2002), explains how the elite that funds the media—either through direct ownership or advertising—and maintains quid pro quo relationships with the makers of “the news” plays a decisive role in the establishment of a hegemonic set of ideas, values and principles. The media works to present them as if they have all the properties necessary for the audience to confidently take for granted their factuality and veracity.

Regardless of whether it does or not—Chomsky and Herman clearly state that results are not homogeneous—this ideation capability is critical to cyber-psycho-

cognitive operations, for it implies that political candidates or legitimized authorities who enjoy the favor of the elite controlling the media can use it to both strengthen the beliefs on which their legitimacy is based and attempt to dismantle those on which their rivals' potential or existing legitimacy rests. As analytical framework, however, the "propaganda model" stops at studying the "media structure and performance (…) [the] forces that shape what the media does" (Chomsky and Herman, 2002, p. XU). It explains neither "how" it does it (i.e., the media's "agency," according to Burke's dramatism), nor "the effects of the media on the public."

I resorted to Maxwell McCombs' agenda-setting theory to explore the media's agency (McCombs, 1994; 2014). Influenced by the structural power exerted by their financial and political supporters, the media configure the content that will be communicated through their channels, using strategic criteria to select "what" out of everything that could possibly be of relevance to the audience will be in fact "covered." Thereafter, a metanarrative about topic predominance is operationalized; by committing airtime, column inches and digital publishing resources to the "representation" of the series of selected topics, there is a concomitant exclusion of all other issues that, in spite of their occurrence in physical reality, no content is ever produced to represent them for the public. This discrimination is the media's implicit statement about what they want the public to regard as "important to know." The topics for which news stories are created conform what is known as "the media agenda." Agenda-setting manifests its first dimension when the audience consumes and discusses these news stories' content, reproducing the predominance of the media agenda topics to the point of turning them into the most salient issues in the public sphere.

However, to McCombs the discursive transfer from the media to the public agenda is not limited to issues or specific stories, therefore, the process should be conceptualized as a conveyance of objects through mediatic channels. This abstraction extends his theory to encompass all kinds of transferable discursive elements, thereby affording the real-life scenario in which objects such as "election campaign," "candidate X," "candidate Y," "email server," "Russian hack" can be transferred from the media to the public agenda. But objects are not transferred as "neutral entities;" agenda-setting's second dimension is defined by the association of attributes to the transferable objects. Thus, if agenda-setting's first dimension performs a function of establishing object salience, the second works to establish the salience

of specific attributes in the definition of agenda objects. For instance, a candidate could have both significant government experience and a history of delivering expensive speeches to bankers. The former conveys what for many is a highly-desirable trait for a presidential candidate: “government experience.” The latter confirms the candidate’s linkages to the financial elite and portrays her as a “greedy” politician. In a political environment where the one common interest between the two strongest forces is their expressed desire to “change the status quo” and “defeat the Establishment,” these could be seen as negative attributes. The media could choose—or be persuaded—to emphasize one of the topics by committing more publishing resources to it and hence support either the construction or destruction of a seemingly “presidentiable” avatar. Whichever the course of action, the media tends to substantiate their emphasis by presenting one or more narratives about how the salient set of attributes has a connection to an issue deemed important in the public debate. The mediatic articulation of this type of media-public agenda relationship is agenda-setting’s third dimension. And the overall scheme whereby the media attempts to make certain attributes have a heavier weight than others in the definition of an object is called “priming.”

A quick look at the cited theories’ years of first publication reveals the fact that the notion of “psychological legitimacy,” the “society of the spectacle,” the “propaganda model” and the media’s agenda-setting function all predate the ICT revolution. In the second section of the third chapter, “Processual Components,” I start describing parallel, artificial-intelligence-based mechanisms performing analogous and complementary processes to those described above. Moreover, the dynamics at this level can elucidate “the effects of the media on the public”—one of the limits that Chomsky and Herman set for the “propaganda model” analytical framework. In other words, they can shed light on how mediatized “representations” of the world and their constructed relationships to individuals’ own perceptions of their environment effectively condition the psycho-cognitive processes through which they legitimize or deny legitimacy to both political figures seeking to become authorities and authorities seeking to remain in power. Yet, as I stated earlier in this section, I lacked the means to carry out the massive, user-information interaction experiment needed to observe these dynamics first-hand. Therefore, my contribution to the topic is limited to a preliminary application of Anthony Giddens’ structuration theory (Giddens, 1984) to

individuals' recursive, belief-construction practice of consuming digitally-mediatized "representations" from sources they trust as "knowledge providers."

I considered structuration theory particularly adequate because the act of searching and disseminating these object-attribute constructs under the assumption that their messages transmit "knowledge" reproduces the data-based conditions that foster their manifestation in the private and public spheres. This is because the spacetime coordinates of their manifestations are dynamically linked to score rankings that improve as a result of content consumption and reproduction. I am referring to search and social media platforms' calculations regarding the object-attributes' contextual relevance vis-à-vis user intent as well as their authorship trustworthiness. "Relevance" is calculated with a bias towards users' places and pages visited, past searches, "likes," comments, shares, friends, followers, people followed and more. Thus, it is a mechanism that organizes every present and future frame of viewable content according to "what has already been." As people can only reproduce what they have seen, and every constituting element in the user experience has its own address (i.e., a Uniform Resource Locator or URL), when they share content online, they reproduce the link to it and increase the chances of the links stemming from the content being shared by their audience as well. The more that a piece of content is referenced in relation to an object-attribute, the higher its relevance score vis-à-vis the topic and, hence, the higher its ranking in the lists of search results produced for queries associated to the topic.

But sources are not all regarded equal. The ones that have the most links from "trusted" sources also have the highest authority rankings, which, by the same token, are considered "trusted" sources of knowledge on the topics they are the most referenced for. This logic tends to create "an ecosystem of 'knowledge' sources" where they are always referencing one another, thereby maintaining their collective status as "the trusted sources of 'knowledge.'" According to search engines and social media platforms' authorship trustworthiness logic, every time that a user searches for a topic, the relevant content from these sources should outrank all other relevant matches in the list of search results. And since they tend to rank the highest, they tend to be the most shared, which leads to the self-reproducing recursion of the social practice of online-based "knowledge" construction. Thus, action and meaning seem bound by the structural constraints generated by the logic of the private algorithms that regulate the primordial spacetime of intersubjective discursive construction.

Other structural conditional mechanisms emerge as a result of the structuration of knowledge construction and reinforce it through their own reproduction. Most notably, the data, information and knowledge dependencies generated by the global knowledge-based economy, also propelled by the private web services and their proprietary algorithms. As mentioned earlier in this section, user-computer interfaces emerged to fulfill the need to facilitate the proper utilization of microchips' computing power and hence operationalize their use in all social activities and contexts. Eventually, these interfaces grew into hierarchical, mostly-interdependent, functional narratives combining physical and virtual inputs (e.g., "if you quickly press the left button of the artefact everyone calls 'mouse' two consecutive times when the arrow figure on the screen is positioned over the small rectangle resembling a button that reads, "Buy Now," the images on the screen will change to show a series of purchase-confirmation messages. You should be getting a package in the mail a few days from then."). The fact that performing the same actions produced the same system behaviors time and again, provided the cognitive conditions for users to assume the validity of narratives' claims. The fast invocation of narratives needed in order to turn computers into effective working tools in industrialized environments would be unattainable without this pre-validation of functional assumptions.

The same holds true for the collective, tacit accord in believing and invoking these functional assumptions; it would be pointless to deploy a fully-computerized production system if only a handful of users actually believed in the idea that, for instance, hitting the "Enter" key produces a user command for the computer. By the same token, for a new member to join a workforce invoking these and other interdependent beliefs he or she must share and apply the same set of beliefs. On the other hand, the pre-existing members do expect for newcomers to believe and play by the same rules, otherwise, they cannot contribute to the collective production tasks that makes their interactions purposeful. Exclusion and self-exclusion would be acceptable outcomes if only these social practices were confined to a definite type of activity, place or time; but they are in fact boundless: they permeate the corporate offices, the manufacturing plants, research centers and all kinds of nonwork activities that can be performed in the public and private spheres. Giddens described this phenomenon decades before it began to fully manifest:

> Human social activities, like some self-reproducing items in nature, are recursive. That is to say, they are not brought into being by social actors but continually recreated by them via the very means whereby they express

> themselves as actors. In and through their activities[,] agents reproduce the conditions that make these activities possible (Giddens, 1984, p. 2).

Just as users rely on other users to share their beliefs regarding the application of functional narratives in respect to computers and information systems, the incorporation of these routines and the data they produce as critical elements at all levels of the production process of most if not all industrial sectors has turned societies dependent on these outputs. Hence the commoditization of data, information and knowledge, the latter giving purpose to the acquisition of the first two, for it is with it that decisions can be made. Therefore, there is a collective demand for knowledge and a common expectation that, once received, it be operationalized through decision-making. Nevertheless, a problem arises when on the one hand, the production of data, information and knowledge becomes so lucrative that its "manufacturing" is performed nonstop, regardless of whether there is anything "new" about what is provided as "knowledge." Or worse, when what is provided as "knowledge" has not gone through the testing and verification processes that would make it so. The problem is exacerbated by the plethora of scenarios in which "knowledge" channels can reach knowledge seekers. This is how the ubiquity and pervasiveness of ICTs functions as instrument in the reproduction of strategic lifeworlds, that may or may not be entirely based on beliefs that correspond to factual information, but steer society towards the construction and maintenance of some type of sociopolitical order all the same.

Through the "See, Think, Do, Care" model for the mapping and orchestration of profitable online "user journeys" designed by Avinash Kaushik (Kaushik, 2015), I explained how deep-learning machines can guide users to develop specific beliefs about their environment in much the same way as they "assist" them in the process of becoming recurrent purchasers and brand-lovers. Kaushik's work is extremely relevant to understanding not only the state of the art in search engines' operational capabilities, but also the logic behind the commoditization of user experiences with web content as a whole. Since its release, Kaushik's user journey digital marketing model and its underlying principles have provided the guiding light for much of the industry, which is partly explained by Google's endorsement of "See, Think, Do, Care" and Kaushik's appointment as the company's digital marketing evangelist (Gallo, 2016). Nevertheless, Kaushik is not the only source on which I based my views on online user-information dynamics. Alike my analysis of the prosumers and the data acquirers and generators presented in the "Political Actors" section, I based my understanding

of user journey machine-learning and the other processual components' operations on a combination of patent and scientific article research, peer-reviewed books, blogs written by expert practitioners and fourteen years of professional experience in the digital marketing industry. During the best part of the past seven years, I worked in various capacities involving the analysis of user-generated content and data, online user experiences and web search dynamics.

Lastly, in chapter four, I complete the integration between the theoretical framework explained above and the case study of the American presidential election of 2016. I begin by explaining the progressive build-up of interdependent functional narratives and their generation of trust towards their consistent behaviors and outputs. This is proceeded by my argument regarding the transition to the formation of trust in the avatars represented online and the political power that this bestows on the real entities they represent. This discussion serves as the preamble to a study that adopts methodological elements from Norman Fairclough's Critical Discourse Analysis (CDA) framework (Fairclough, 1995), including the observation of characteristics of language and word use, and the description of objects, attributes, central terms and communication motives. Through a cumulative process of discovery and revision of mediatized text, I put forth message observations as evidence connecting the media, the State and the parties' discourse to the body of theory discussed here.

Given the incipient state of the overarching theoretical project being envisioned, this dissertation placed especial emphasis on the case study's spoken and written language text, as well as in the political and cybernetic mechanisms involved in the processes of production, distribution and consumption of political discourse. Although the analysis of events in the light of well-established theories generated the scientific conditions necessary for the confident formulation of some abstractions, the task of testing their generalizability will require further elaboration. Among other things, this will most likely entail incorporating the comparative analysis of other case studies on the topic and reinforcing the abstractions' empirical foundations with first- and second-hand experiments designed to obtain hard data. For the time being, I believe the reader will find this inductive analysis to be a solid starting-point.

2. THE ACCIDENTED ROAD TO THE CURRENT PARADIGM: ECONOMY-DRIVEN PROLIFERATION OF ICTs' USERS AND USES

If the chances of a latent threat's realization increase with the proliferation of the material inputs required for its manifestation, then curtailing the production or spread of such materials could lead to a decrease in the likelihood of its actualization. If the Russian party that performed the pre-election psychological operation of 2016 owes its success in large part to the degree of ICT devices' and functionalities' societal spatiotemporal penetration, then, it would seem logical to consider that curtailing their proliferation would also reduce the chances of a new social hack taking place. But, could such strategy be actually implemented? To examine the case of ICTs, it is worth making a brief detour into a *problematique* in which there is a similar connection between the variables of material input availability, proliferation and threat degree. Obvious ontological, effectual and consequential differences notwithstanding, the international freeze in nuclear warhead proliferation and its impact in nuclear war threat reduction provides one such example.

The belief that nuclear proliferation increases the likelihood of interstate conflict has been a common premise in nonproliferation discourse (Cohen, 2016), at the heart of which lies the assumption that proliferation can be halted. While the belief may not have been fully substantiated yet (Cohen, 2016, p. 425), the assumption has been proven correct. The overall cost of production, the total cost of ownership and the know-how required to build and maintain a nuclear arsenal have been decisive to the implementation of the nuclear freeze on a global scale. Known-how availability notwithstanding, this would seem to indicate that economic constraints can be leveraged to reduce threats whose realization is highly contingent upon the continuous existence of specific material means, when their acquisition is or is made to be partially or fully unattainable for most countries (Joseph S. Nye, 1992).

It is abundantly clear that in spite of scarcity conditions, global nuclear proliferation remained on a steady rise until it plummeted at the end of the Cold War; a token of the vital role that geopolitics plays in the *problematique*. There is also no doubt that whatever success nonproliferation has enjoyed it owes it to more than just the sheer scarcity of the material inputs that countries need to sustain nuclear military capabilities. Nevertheless, economic constraints have imposed restrictions without

which the spread of nuclear arsenals could have happened at a much faster pace and on a broader scale than it did. Then, putting in place the political safeguards necessary to ensure minimum international security standards in the face of proliferation would have been much more difficult to achieve (Daddario, 1977).

Thus, the question arises: could economic factors be brought to bear in the de facto reduction of other threats to global security whose realization may be similarly dependent on specific material conditions? In this sense, if analytical priorities were arranged according to threat recency and novelty, Obama's executive order claiming that ICTs had been used to carry out what amounted to a foreign aggression against the U.S. would place cyberspace at the top of the list of theatres of war requiring close examination. Lest we forget, the alleged cyberattacks under discussion led to the greatest rift in U.S.-Russia relations since the end of the Cold War; a state which certainly brings the world closer to the unwanted scenario of a major international conflict. Could such threat be subjected to a de facto weakening utilizing economic leverage points using the same logic underlying nuclear proliferation freeze?

At a glance, there appears to be a fundamental flaw in the analytical inquiry: Weren't the attacks the U.S. was a victim of virtual in nature? If the economic constraints that have so far curbed nuclear proliferation are intimately linked to the material quality of the threat's means of realization, then how would a threat whose means of realization are essentially immaterial qualify to establish a valid comparative framework? Logically speaking, wouldn't this be a form of faulty comparison?

It would not, for at the most basic level, cyberspace is a flow of data transfers that occur over a robust and sophisticated network of material infrastructure and devices capable of producing, sending and receiving data (Strate, 1999). In other words, it is these material components that make the publishing of unverified content possible. In fact, there would have been no instruments to produce, send and receive any of the messages that not only made the image of an otherwise successful career politician gradually wither away, but also plunged a nation into an escalating process of Weltanschauung-based sociopolitical fragmentation and violent turmoil. Then, on election day, perhaps the hearts and minds of voters in former bastions of the Democratic party would have been in the right place to help her win the 270 electoral college votes that she needed to secure the presidency.

According to an FBI-DHS joint report (Federal Bureau of Investigation and U.S. Department of Homeland Security, 2016), the aggression was two-fold: a series of

cyber-intrusions into both the Pentagon and the private computers of individuals with direct or indirect ties to the federal state, and a campaign geared towards the destruction of the image of the elite's favorite candidate. First, hackers purportedly syphoned a combination of federal and private documents, and second, they utilized the data contained in some of these documents to configure a targeted cyber-psycho-cognitive operation on various key segments of the American electorate. While the intrusion was considered an aggression in and of itself, it is what was carried out with the data obtained from the break-in that brought the destructive consequences that gave substance and significance to the intrusion. It is also in the technological aspects that made this psychological operation viable that lies the key to understanding how, unlike in the case of nuclear weapons, economics plays a propellent role vis-à-vis the proliferation of ICT devices and the legitimacy-corroding narratives they can produce—the material and immaterial means of destruction.

Essentially, the reason why economic forces have contributed to, rather than forestalled, the proliferation of ICT devices is because they are both the means of production and the products of self-reinforcing, innovation cycles (Manimala, 2009), comprehending, on the one hand, the production and enhancement of ICT devices' and, on the other, data's functional capabilities and the increasing consumption of the cycle's upgraded material and immaterial products (Kuhn, 1996; Harvey, 2003; Fuchs, 2008b). The combined effect of these forces gives rise to a paradigm whose epistemological, technological, cultural and socioeconomic conditions tend to foster iterative, compounded upgrades in not only the ICT artefacts, but also in the knowledge they facilitate the production of and the processes through which they do so. This generates the conditions for an endless, continuous cycle of exponential improvement at the heart of which lies a synergy among a myriad of technological and economic factors inherent to ICT innovation.

Given the fact that each innovation cycle builds upon the advancements of the last, I deemed a genealogical approach to be most suitable for the task of providing an explanation of these synergic dynamics. Nevertheless, the material and immaterial aspects conditioning ICTs' innovation cycle can be synthesized as follows: (1) the inverse relationship among the microprocessor's shrinking size and its increasing computational power, which has made the spatiotemporal expansion of ubiquitous computing possible; (2) the declining cost and price of upgraded microprocessors, which has enabled the exponential growth of ICTs' user base, encompassing large

segments across most social strata; (3) hardware and software scalability, which facilitate systems and networks incorporation of additional resources with which output capacity can be more easily adjusted in order to adapt to tasks of increasing complexity; (4) data's capacities to be obtained, edited, reused, reproduced and repurposed by individuals and systems across devices, applications and environments, which, by enabling selective collaboration across time-space boundaries, increase the pace of knowledge generation, validation and acquisition.

Unfortunately, the same data qualities that accelerate the pace of knowledge articulation and integration also create the conditions that make possible the production and dissemination of false information posing as "knowledge." When strictly considering the processes of scientific and technological innovation, the final impact of "false knowledge" is minimized through well-established testing and verification procedures. However, information production activities in fields where scientific testing and verification are not *sine qua non* conditions (i.e., journalism) have been rendered more vulnerable to its detrimental effects. Part of the problem is that, unlike the information that propels ICT artefacts' innovation, where only true knowledge can generate utilities (Rice and Giles, 2017), the information used to produce cyberspace content does not need to be true for it to generate capital (Fuchs, 2008a; 2011). Here, capital is generated through information reproduction and consumption; viewing and clicking suffice to generate profits. The dynamics and mechanisms underlying this phenomenon, as well as the material and immaterial factors at play in the trajectory of ICT innovation will be henceforth explained following a loose chronological order.

The scientific and cultural origins of the informational paradigm lie in the point of convergence of two rather antagonistic types of agents: the European and American military apparatuses and the hippie countercultural movement of the 60s (Castells, 2010b, p. 49 - 50). Innovations in computational science oriented to derive strategic advantages were developed with the sponsorship of the militaries engaged in World War II (Mahoney, 1988). In 1943, these advances evolved into ENIAC; the first complete, programmable computer for general use (Shurkin, 1996). It had, nevertheless, one major inconvenience: due to the number of components it needed to make its computations, it was a large piece of hardware; it spanned an area equivalent to 1,800 square feet. In 1957, Jack Kilby set out to solve the size problem. He created a single "a body of semiconductor material […] wherein all the components of the electronic circuit are completely integrated" (Winston, 1998, p. 221), thus, the

first integrated circuit was born. Six months later, Robert Noyce would make an integrated circuit that was different from Kilby's in an aspect that would prove to be critical. He substituted Kilby's germanium-made chip with a small silicon wafer whose conductive properties had been altered through controlled oxidation in order to electrically isolate the chip's transistors, thus enabling their operational independence while being interconnected through the semiconductor material (Noyce, 1977; Lehovec, 1978). However, besides enabling this electric isolation effect, the controlled oxidation process also altered the relationship between the transistors' power density and size such that the former remained constant even when the latter decreased; a phenomenon explained by Dennard's scaling law (Dennard *et al.*, 1974).

Therefore, the components embedded onto Noyce's silicon wafers could engage in separate functions thanks to their independence and the area occupied by each could shrink without it affecting their power output. In other words, as silicon wafers could pack an increasing number of components—transistors, resistors, diodes or capacitors—their power could remain unchanged even as they got smaller. This had vast implications for the emerging industry, many of which were summarized in what would become one of most influential papers in the history of IT, published in 1965 and written by Noyce's colleague and co-founder of Intel Corporation, Gordon E. Moore; "Cramming more components onto integrated circuits." He forecasted that the number of components that could be crammed onto a square inch of silicon would double every year, leading to a simultaneous fall in the unit cost (Moore, 1965, p. 114). Thus, this extended the inverse relationship between power density and size also developed an inverse relationship between power density and cost.

When integrated circuits began to contain central processing units (CPUs) the performative and economic advantages entailed in these relationships cascaded to computers and, hence, to the entire IT industry. This explains the steady 16% average annual fall in computers' prices vis-à-vis performative quality that began in 1959 and lasted until 2010. In fact, from 1995 through 1999, the pace of the price fall accelerated further, reaching 23% per year. In recent years, however, the decline has slowed down to a 2% annual average. (Aizcorbe *et al.*, 2006; Nambiar and Poess, 2011; U.S. Bureau of Economic Analysis, 2018).

But while the size, pricing and computational power of microprocessors are still three of the key factors driving the continuous expansion of cyberspace, they cannot account for ICT proliferation on their own. There is no question that productivity gains

stemming from computational-driven, task and process automatization paved the way for the digitalization of the work environment across all industries. However, the motivation to adopt microcomputers into the intimacy of social life did not come from the fact that they were workhorses being sold at increasingly affordable prices. To comprehend the phenomenon in its full scale, a return to the question of how computer hardware was socialized is in order.

One thing should be stated from the outset: although their functionalities responded to socio-industrial challenges, there were mixed views as to the extent of computers' "people friendliness" (Hirschheim, 1986). Despite their practical potential, the first microcomputers were seen as bulky, costly, fragile—even frightening—working tools (Rosen, 1969; Seidel *et al.*, 1982, p. 61-62; Kildall, 1985; Strassmann, 1985; Grundy and Grundy, 1996, p. 26; Bosker, 2013; Lean, 2016). They were not the kind of article that on a new model's launch-day eve people would camp out around the store to be the first to purchase. Though the day when hundreds of people would do this kind of willful sacrifice was beyond the horizon, Steve Jobs and Steve Wozniak would take the world a step closer in this direction at the 1977 West Coast Computer Faire. This was the event in which where their company, Apple Computers Inc. launched the first consumer-market, household-style, personal computer: The Apple II.

Building on the idea of providing instruments for people to easily harness microprocessors' computational power, Jobs and Wozniak delivered a user-oriented, physical interface comprised of a keyboard embedded in a plastic case inside of which was the machine's circuitry. Implicit in the system's design was an emerging notion of human-computer relationship, whereby the machine provided the user with intuitive input mechanisms to direct its performance as either a calculating machine, or a word processor. This concept was taken a few steps further with Apple II's successor, the Macintosh, which was the first mass-market computer to incorporate a Graphical User Interface (GUI) displayed over a built-in, black-and-white monitor. The system also included a keyboard, a mouse, and a floppy drive that took 400 kB 3.5" disks. From now on, the tiny microprocessor would have clear interaction instruments with which users from a broad spectrum of society could harness its power (Atkinson, 2007). By becoming usable to more than just computer hobbyists, microcomputers could now serve a function beyond the corporate office, in the homes of millions of users whom, through their adoption in everyday life, would give them new and richer meanings

(Atkinson, 1998; 2000). This of course enlarged the universe of social activities and spaces deriving the computer market's needs and wants; two of the IT industry's strongest directive and propelling forces (Stein, 2011).

Needless to say, hardware was not the sole advancing front. Increments in computational power and socioeconomic adoption led to increasing utility potential and new social purposes waiting to be fulfilled (Grudin, 1990). This shed light on the fact that much of the microprocessor's technological capacity would remain idle until usable and intuitive tools were devised to tap into it (Kleinrock, 1967). For the experience of interacting with a computer to be meaningful, the agent needed to observe a graphic representation of the inputs and outputs resulting from his/her interactions with the computer (Tourangeau *et al.*, 2003). Built-in monitors, keyboards and mice were the peripherals with which such interaction could be possible, but what could or should be the expected outcome of this interaction?

The user could only evaluate the effects on his/her peripheral-mediated actions through their visual manifestations on the monitor's screen (Grudin, 2012). It is in the human-computer interactions' graphical effect "compositions" that lies the value of the time and effort required to establish such synergetic experience (Barr *et al.*, 2002; Barr, 2003; Barr *et al.*, 2004). The moment in which these creations can be losslessly stored as intangible objects for future unattenuated retrieval (i.e., data) they gain the potential to transmit knowledge. Moreover, knowledge can derive information, which, in turn, is an input in the decision-making processes that guide human activity (Proctor and Vu, 2012). Therefore, taken together, the data storing knowledge representations also store the value of knowledge vis-à-vis decision-making. Fundamentally, this is how the advent of technologies capable of representing, transmitting and storing knowledge has led to its commodification.

Vital to the process of harnessing the computing power of microprocessors for knowledge production are the graphical abstractions to which users apply their inputs on the screen. Stemming from the idea that promoted the design of hardware to support user interaction, the invention of graphical user interfaces (GUIs) came as a response to the steep learning curve that command-line interfaces (CLIs) posed for the average user (Engelbart, 1962; 2008). They were a series of metaphors designed to facilitate rapid, reversible and incremental human-computer interactions through the direct manipulation of continuously represented objects of interest ranging from layout organization elements to graphical icons and indicators. Backed by funding secured

by National Aeronautics and Space Administration (NASA) program manager Robert Taylor, Douglas Engelbart and his team of engineers at the Stanford Research Institute's Augmentation Research Center began devising GUIs since the early 1960s. Their public debut occurred on December 9, 1968 at that year's Fall Joint Computer Conference in San Francisco, an event since then dubbed "The Mother of All Demos" (Engelbart, 1968). In front of a large audience, Engelbart presented the "oN-LINE System" (NLS); a multi-user collaboration software suite pioneering many concepts and objects that would serve as the basis for today's human-computer interface standards: bitmapped video monitors, the mouse, the practical use of hypertext links, relevance-based information hierarchies and windowing behaviors.

GUIs were seen as the future of computing precisely because they afforded the execution of human requests of varying degrees of complexity through relatively simple and intuitive visual elements and human-machine choreographies. While this minimized the user's conceptual awareness of the operating system, it also maximized the utility of peripheral instruments—otherwise limited by their objective physical interaction mechanisms—vis-à-vis the system's behavioral performance. Eleven years later, Apple Computers would popularize the so-called "desktop metaphor" through the Classic Mac OS, which was released as the Apple Macintosh's hardware and software resource manager (Vertelney *et al.*, 1993; Reimer, 2005).

By the mid-1980s, the IT industry had developed all the elements required to enter a paradigm of self-sustainable innovation. On the one hand, it had established an inverse relationship between increasing computational capacity and efficiency and, on the other, it had managed to maintain microcomputers' decreasing manufacturing costs and prices (Cohn and Haddad, 1986). It had begun a continuous improvement cycle, which had led to a relentless industrial incorporation drive, and an expansive adoption in everyday life (Vitalari *et al.*, 1985). Software innovation had also started to be acknowledged as a mission-critical factor, whereby the existence of idle computational resources and greater storage capacities could afford much needed enhancements in both software performance and quality. The resulting boom in software development would eventually lead to the ongoing trend in which computer programs' soaring degrees of robustness and sophistication exhaust and exceed hardware's computational capacity faster than it can increase it (Ecker *et al.*, 2009). Henceforth, software feature enrichment became one of the main driving factors propelling hardware innovation. This synergy between the hardware and software

sectors would eventually lead to a sustain demand for the consumption of ever more sophisticated and specialized computer-mediated experiences which characterizes the current order. But the massification of this demand could only occur as a result of a phenomenon which began brewing in computer labs at the U.S. Department of Defense Advanced Research Projects Agency (ARPA), the University of California, Los Angeles (UCLA) and Stanford University during the early 1960s: The Internet.

In fact, graphical user interfaces and computer networking emerged as two parts of a solution to the economic and technological problem of popularizing the use of computers in a time when only large universities and corporations had the resources to purchase them. GUIs provided a virtual context for users' direct manipulation of computer resources that maximized the impact of the few kinds of physical inputs at their disposal vis-à-vis computing throughput. Nevertheless, in the early years of microcomputing, this interaction model was still insufficient to exhaust the computational capacity available when applied in the context of a one-to-one, human-computer relationship. In part, this was due to the idle time lapses that would take place between one moment of constant input to the next. Thus, an expensive piece of equipment was being underutilized. This represented both an additional obstacle and a dilemma for the academic and scientific communities. On the one hand, paying a high price for a resource that no one was able to efficiently utilize did not seem to be a wise investment. Yet, on the other hand, it was clear that computers had a great potential to facilitate dramatic improvements in all stages of the research process. Due to this, adoption seemed as desirable as inevitable.

The academic and scientific communities responded by devising a utilization method that would allow several users to concurrently access the same computer's resources through input/output equipment based in their premises. This is how the concept of "time-sharing" was born; one single computer would manage many information requests from many users, thereby utilizing each lapse of computing time available (Corbató *et al.*, 1962; Chvany, 1972). Then, it is no coincidence that several of the key stakeholders in the institutionalization of time-sharing as the prevailing computing model also played pivotal roles in bringing GUIs from concept to industrial production, most notably Joseph Carl Robnett Licklider and Robert Taylor.

Seldom have a scientist's writings foreshadowed a historical paradigm with as much accuracy as Licklider's, "Man-Computer Symbiosis" (Licklider, 1960), "On-line Man-Computer Communication" (Licklider and Clark, 1962) and his "Memorandum For

Members and Affiliates of the Intergalactic Computer Network" of April 23, 1963 (Licklider, 1963). Together, they read as a blueprint of the information society we know today. This, too, is no coincidence; both works had eureka effects on a collection of individuals whose academic backgrounds allowed them to see the great scientific potential endowed in Licklider's vision. Furthermore, through their government connections, some of these individuals had access to valuable resources which they were able to commit to the materialization of this vision. This is how distinguished electrical engineer and Director of the Advanced Research Projects Agency (ARPA)[4], Jack Ruina, brought Licklider on board as the first administrator of the Information Processing Techniques Office (IPTO). He saw Licklider's "Intergalactic Computer Network" as the answer to a threat besieging the U.S. since the beginning of the Cold War: that a successful nuclear attack on the homeland could bring about the total collapse of the government's and the military's communications capabilities, thereby rendering the country's defenses inoperative.

It was during his tenure at ARPA that Licklider met Robert Taylor, who had been investing a portion of NASA's budget in Engelbart's GUI research since the early 60s and who had also come to develop a special appreciation for Licklider's "Man-Computer Symbiosis." Three years later, he would have the chance to further the implementation of Licklider's vision as the new head of the IPTO. During his time as director, the IPTO furthered three of Licklider's most transcendental contributions to information technology: time-sharing, networking and the creation and funding of the first computer science departments at major American universities such as Stanford University, Carnegie Mellon University, the University of Utah, the University of California, Los Angeles and Berkeley, and the Massachusetts Institute of Technology (Mowery and Langlois, 1996; Abramson *et al.*, 1997, p. 229; Ceruzzi, 2003, p. 259). Additionally, besides increasing the Pentagon's investment in GUI research, Taylor also embarked in the creation of ARPANET, the Internet's precursor—inspired by Licklider's "Intergalactic Computer Network" concept.

Through ARPANET, ARPA was to pursue the goal of developing a communication network capable of functioning in the aftermath of a nuclear attack. In a sense, the diversity and congruence between and among the constellation of

[4] ARPA was President Dwight Eisenhower's attempt at bringing the United States up to speed with the Soviet Union, whose successful launch of the Sputnik satellite in 1957 appeared to have given the Soviets a head start in the so-called "space race."

scientific inventions and discoveries brought to bear in its creation attests to the existence of an incipient informational paradigm. Licklider himself seems to recognize that his “Intergalactic Computer Network” concept represents the outcome of such alignment (Licklider, 1963, p. 1). And for every problem he identified in his memorandum, ARPANET’s chief Taylor would find someone who already had a solution for it, or who was working on finding one. This is how he recruited electrical engineer Lawrence Roberts, whom, with the help of fellow physicist, Wesley Clark, was able to design a conceptual model for decentralized computer communications. His network scheme proposed the setup of node-based, nonshared computers dedicated solely to the function of routing data to their intended destinations. These transit facilitators came to be known as “Interface Message Processors” (IMPs), created by a team of engineers including Frank Heart, Robert Kahn, Severo Ornstein, Dave Walden and Willy Crowther (Heart *et al.*, 1970).

Having established this as a potential solution, Roberts sought to find a communications technology capable of accommodating multi-user, online interactivity. Then predominant circuit-switched networks were capable of managing interactive communications such as phone calls. However, their dependence on expensive infrastructural components, as well as their requirement to secure both a specific channel and pre-allocated bandwidth for an entire call or session made them inadequate to sustain a totally survivable system containing no critical central components, which was ARPA’s primary goal. Moreover, since interactive data traffic occurs in short streams, call- or session-based bandwidth pre-allocation led to bandwidth wastage rates of 90 percent and above. Therefore, circuit-switched networks were unfit to support intermittent communication processes in a cost-effective manner. These contextual conditions made Roberts look for a solution elsewhere.

During the course of his survey, Roberts became acquainted with a eleven-volume study on “distributed adaptive message block switching” carried out under contract to the U.S. Air Force through the RAND Corporation (Baran, 1964). The author, RAND electrical engineer Paul Baran, had created an interactive data communication method which, instead of securing a specific channel and pre-allocating bandwidth for entire communication processes at a time, relied on the transmission of small data packets using dynamically allocated resources. Hence emerged what was to become ARPANET’s underlying data communications technology: packet switching. Besides disposing of the requirement to secure a

committed transmission route and bandwidth, packet switching allowed for the allocation of transmission resources one block of data over one network link at a time. From any given point “A,” data packets could travel through many different paths to reach point “B,” which ensured that knocking out a part of the network would not accomplish the total collapse of communication between and among peers; hence, the solution seemed to effectively address the Pentagon’s main concern. Besides permitting the fulfillment of the network resilience requirement, packet switching also afforded the flow of concurrent, multi-user, sending and receiving processes without increasing transmission resource consumption. Thus, packet switching became the most cost-effective method of interactive communication, outperforming circuit switching in its potential for reducing transmission bandwidth. According to Roberts, “depending on the nature of the data traffic being transferred, the packet-switching approach is 3-100 times more efficient than pre-allocation techniques in reducing the wastage of available transmission bandwidth resources” (Roberts, 1978, p. 1307).

Paradoxically, for all practical purposes, the U.S. Air Force ignored Baran’s work. It took several years for packet switching to resurface as a topic of discussion in the Pentagon. And even then, the concept was brought back to the fore not after revisiting Baran’s research but rather, after Roberts became acquainted with the work of Donald Davies, a Welsh mathematician and computer scientist working for the United Kingdom’s National Physical Laboratory (NPL). Their encounter came as a result of Davies’ interest in one of the university-based, time-sharing projects that ARPA was funding at the time: the MIT’s “Project on Mathematics and Computation” (Project MAC). Davies arranged a seminar at the NPL headquarters in London on November 2 and 3 of 1965. Roberts and some of the MIT scientists involved in Project MAC were among the attendees. It was at this meeting that they began discussing the fundamental challenge of, in Davies own words, “how you could get hour-long telephone calls in which not very much data was transmitted; what you could do about making communications more efficient” (Pelkey, 2007).

It was studying this time-sharing computer system that Davies arrived at essentially the same conclusions that Baran had five years earlier. He realized that humans interact with computers in “bursts;” they input data, stop to think what to do next, provide more input, think some more and so on. Davies figured that due to this interaction-thinking dynamics, interactive computing led to great degrees of both computing and bandwidth underutilization. Furthermore, this intermittent user demand

pattern made access to time-sharing computers via long-distance telephone lines costly to the point of being unaffordable to most people. Nevertheless, since time-sharing had proven to maximize hardware utility, it was plausible that the same principle could yield similar results when applied to data communications. Hence, the engineering challenge Davies set out to face was the production of a data transmission method with which the sharing of computing resources could coexist with the sharing of data transmission resources. The result—which he named “packet switching”—not only accomplished this coexistence, but also empowered the generation of multiple, simultaneous user experiences characterized by continuous, immediate responsiveness, thereby enhancing the quality of computing interactivity for entire networks at a time. A highly sophisticated product for what can be simply explained as the technique by which a single data transmission line could be shared among many users by concurrently transmitting their inputs in small data packets (Campbell-Kelly, 2008).

As significant as Baran’s and Davies’ advancements were in bringing ARPANET closer to the realization of Licklider’s Intergalactic Network, there were, to be sure, many challenges ahead. First came the need to conceptualize a model for the sending and receiving of data among networks prone to several forms of heterogeneity; from endogenous configuration specificities, to the nature of their mediums, as the goal was to integrate satellite, radio and computer networks. Second was the contradiction of having to engineer a solution that could provide the normalization necessary for internetwork data communications across different types of networks, while avoiding a generalized, intra-network uniformization. The problem with this was that it would condition entity participation to their conformation to a given standard, thereby placing a logistical obstacle to network survivability and expansion, while also limiting network management independence. The third challenge was delivering this as a common protocol, oblivious to endogenous network specificities, capable of masking the mechanisms integrating multi-type, internetwork data communications. This concealment was to ensure the construction of a seamless interactive experience.

The creation of the data communications solution meeting the aforementioned requirements was possible thanks to the work of scientists such as Louis Pouzin, Robert Kahn and Vinton Cerf, whose efforts produced the datagram (the basic unit in a packet switching process) and the TCP/IP protocol suite (both the conceptual model and the set of common communicational procedures regulating internetwork data

packetization, addressing, transmission, routing, and reception) (Pouzin, 1973; Cerf and Kahn, 1974). Complexities were abstracted and simplified, and their underlying requirements distributed along four levels of abstraction. This layered architecture conceptually encapsulates numerous families of specialized, independent methods addressing distinct, yet related data communications functionalities and purposes. The Internet is one of these four layers; the one dedicated to the protocols that handle the end-to-end transport of data packages across networks.

The World Wide Web (WWW) is, on the other hand, an information space comprised of files residing at specific memory locations in host computers capable of sending their constituting data packets when a client prompts them to using the data communications methods stipulated in the TCP/IP protocol suite (Berners-Lee, 1999). This interaction usually involves an application through which the user places the file requests using their addresses in the hosts' memories, that is, their "Uniform Resource Locators" (URLs). Although the function of fetching files from hosts is not exclusive to them, the one type of application for which this function provides its purpose is called "web browser." To communicate with the servers hosting the files, web browsers utilize the methods declared in the protocols of the Internet protocol suite's application layer.

A prime example of this type of protocol is the one that defines the methods that web browsers must execute in order to exchange and transfer hypermedia resources on the WWW: The Hypertext Transfer Protocol (HTTP). These hypermedia resources include text, graphics, video, audio, as well as the hyperlinks referencing the documents storing the data they are made of. Hypermedia elements are the building blocks of users' online experiences and their manifestation on web browsers is made possible thanks to the HTTP. It is for his creation of the first web browser and the HTTP that Tim Berners-Lee is considered the father of the World Wide Web, which today is cyberspace's primordial realm of social interaction. And cyberspace does seem to bear the marks of the creator's original vision for the Web—which reads like a passage taken out of Licklider's Intergalactic Network (Licklider, 1963):

> Suppose all the information stored on computers everywhere were linked, I thought. Suppose I could program my computer to create a space in which anything could be linked to anything. All the bits of information in every computer at CERN, and on the planet, would be available to me and to anyone else. There would be a single, global information space (Berners-Lee, 1999, p. 4).

Judging by the present state of affairs, it would seem as if cyberspace is indeed the fruit of a well-supervised growing process. However, back in the early 90s, Berners-

Lee and all other parties involved in the making and expansion of the Web had yet to develop the information structures and algorithms that would eventually make it transcend its existence as an open portal, whereby clicking a link led to another portal with many more links to other portals. He had taken the first step towards freedom from the epistemological preconditioning imposed by rigid information hierarchies guiding knowledge construction. He had planted the seed for nonlinear learning deploying the tools for the articulation of a space in which ideas appear on the screen in a fashion so emergent that it mirrored the mind's own behavior (Berners-Lee, 1999).

But back when the web had just began becoming pervasive, the meaning of the words displayed on the screen could only be understood by the user; machines could tell whether two words were the same given that, at the binary code level, they represented just specific sequential character arrangements. Grasping the semantics of such sequences was a whole different challenge; one that needed to be taken up before machines could serve the purpose of actively assisting humans' nonlinear learning processes. This was, after all, Berners-Lee's primary goal when he set out to devise a method to document and retrieve information describing the connections between his fellow researchers and their most relevant defining attributes. And soon after the Web was flooded with documents referring to all sorts of topics, computers' inability to compute semantics acquired concrete, real-life quandaries: the web had already become a sea of information but most of it was irrelevant vis-à-vis an individual's interests at any given point in time, how does a user find what is currently relevant to him/her in a sea of irrelevant information? Search engines—information systems dedicated to finding information on the WWW upon request—were built to solve this shortcoming. More than solutions, however, their output shed light on the root and true dimension of the underlying problem; for all practical purposes, their search results were mostly information dumps containing a few web page listings pointing to somewhat relevant sources, mixed with hundreds of false positives. This evidenced the fact that search engines' algorithms were still incapable of discriminating results based on user interests (Lawrence and Giles, 1998; 1999).

Search engines would only begin to develop such capabilities after the mid-1990s, when researchers from various institutions realized that if web files were to incorporate references with which they could be classified, they could be as findable as books in library. In fact, in much the same way as library index cards characterize literary works through a series of common types of attributes, web files would come to

include machine-readable, “data about their data”—metainformation. Then, search engines would play the same role as librarians, facilitating users’ searches for information about specific topics. Nevertheless, depending on both meta-tagging conventions and the engine’s search algorithms, single-hierarchy classification logic could end up dictating search results lists’ content and structure. The danger with this was the hindering of nonlinear learning processes, wherein knowledge is constructed through sequences of emergent discoveries that oftentimes occur while there is little a priori knowledge of the subject matter. If results were anchored to single-hierarchy classifications, their emergence would be rendered contingent upon the user’s a priori knowledge of the keywords that could trigger their inclusion in search results lists. This would then defeat the purpose of having a space for nonlinear knowledge construction, which, as stated earlier, was one of Berners-Lee’s primary goals for the World Wide Web.

Fortunately, library science had long produced faceted classification techniques, which organize information elements by associating them with semantic categories that are combined to form cohesive conceptual expressions (Ranganathan, 2006). Thus, while faceted classification schemes are scalable, flexible, complex and dynamic, their classifying semantic chains can derive exhaustive, specific and exclusive characterizations. This type of classification system played a foundational role in the initial construction of the Resource Description Framework (RDF), a specification outlining the data formats, exchange protocols, conceptual modeling methods, syntax notations and data serialization formats applicable to web resource information across applications, enterprise systems and online communities (World Wide Web Consortium, 1999).

Furthermore, it was the implementation of the RDF standards that propelled the successful expansion of the Semantic Web, which extended the World Wide Web’s capacity not only as a participatory information space, but also as a provider of knowledge that machines could consume, understand and share among themselves. And, as was the case with most other key inventions in cyberspace’s trajectory, the U.S. Advanced Research Projects Agency’s—by then renamed as the “Defense Advanced Research Projects Agency” (DARPA)—sponsorship was key to the success of the Semantic Web initiative.

This was the technological context in which Sergey Brin and Larry Page built “Google, a prototype of a large-scale search engine which makes heavy use of the

structure present in hypertext […] designed to crawl and index the Web efficiently and produce much more satisfying search results than existing systems" (Brin and Page, 1998). Little did they know that their school research project would set a landmark in web searching's underlying logic and user experience, let alone in the individual and collective processes involved in the construction of belief.

This was due to the quantum improvements that Google's 1999 release brought to the degree of congruence between search results' relevance and users' search intents. This, in turn, increased public confidence and search engine usage, leading to the societal validation of the public view of Google as a reliable portal to relevant information. By association, the websites that appeared listed in Google's search results were also regarded as the ones that offered the most relevant content vis-à-vis user search intent. Increases in public trust and reliance on Google as a quality information portal also provoked the mushrooming of online channels to well-established brands from all industry sectors, including the news industry (Pan *et al.*, 2007).

While boosting the web's expansion, these trends created the business opportunity to sell advertisement space to website owners seeking to increase traffic to their websites. Although initially Brin and Page avoided taking advantage of this opportunity, eventually they gave in because there seemed to be no other way of keeping their operation afloat. The compromised they made was that they would have advertising content obey to the overarching logic of granting the greatest chance of visual exposure to the information that proved to be most relevant to individuals' interests at the time of executing their searches. This relevance would be established based on the keywords that users would choose to submit for their queries (Vise, 2006; Sutherland, 2012; Docherty, 2017).

Moreover, advertisers could not buy advertising space directly, nor could they negotiate fixed prices per ad or trigger keyword (Collison *et al.*, 2007; Feldman *et al.*, 2008). Ad impression would work as an auction that would take place every time a user submits a search query (Sharma, 2007). Advertisers would place bids on keywords of their choosing, but the final price to be paid would be calculated considering not only the advertiser's offer, but also a factor that Brin and Page named, "quality score" (Teng *et al.*, 2017). This was a grade in a scale from 1 to 10 which Google assigned based on its evaluation of the ad's and the landing page's relevance vis-à-vis the keyword that triggered the ad impression. Essentially, the highest the

quality score, the lower the final price that the advertiser would have to pay. Furthermore, advertisers could choose to pay either for clicks on their ads, or for one thousand viewable ad impressions (Docherty, 2017).

Since each brand, business, product or service has a set of keywords that best represents it, it is also these keywords that can increase the advertiser's chances of getting clicks from people in his or her market. By making ad impressions dependent on search query keywords, Google ensured that ads would only appear in front of audiences actively looking for the advertised goods, which also increased the likelihood that ad clicks could lead to actual purchases (Sharma, 2007; Weissman and Elbaz, 2010; Hubinette, 2013; Guha *et al.*, 2014; Zhao and Fu, 2016). Nevertheless, there were only ten available ad slots on Google's search results page, which meant that most times advertisers would have to compete for ad space, especially if their goal was for their ads to appear on the page sections with the highest visibility. Depending on the circumstances, it was possible that some of the competing advertisers might have never won one of the ten impression slots.

As the act of searching online for information about anything in the physical world became the norm, brands and companies—and eventually people too—accelerated the pace at which they created and improved their web representations of themselves (i.e. websites, blogs, microblogs and other kinds of online channels) (Castells, 2010a). But for these representations to directly or indirectly generate some form of financial return, they needed to be findable in Google. While paid search advertising was an affordable option for many, the limited "page real estate" available made it increasingly competitive, which imposed hikes in the minimum bid amounts necessary to earn one of the ten ad spaces. Therefore, making content modifications that could yield high rankings on the search results' page appeared to be a necessary investment.

By then, however, it was clear that two phenomena had become a part of the "normal" social order: on the one hand, the practice of using Google to find information about anything in the physical world had become institutionalized, on the other, this pervasive cultural trend had led a significant segment of society to develop the expectation of being able to find everything online (Pan *et al.*, 2007). This resulted in the accelerated online proliferation of digitized, "real world" entities (Poletti and Rak, 2014) seeking to be found. Thus, what began as a new expectation placed upon the experience of reality became assimilated as a fact: so many brands, businesses,

institutions and people created online manifestations of themselves that the online world became a faithful representation of the reality of the physical world. If an entity existed online, its existence could be recognized, else, it could become “irrelevant,” that is, virtually “inexistent.” I would argue that this ontological phenomenon is essentially a product of Guy Debord’s “Society of the Spectacle” in the post-ICT-revolution paradigm (Debord, 1992).

This led businesses to seek techniques that could ensure the permanence of their digital properties’ listings within the first fold of the search results’ page, that is, the screen region spanning the user’s initial field of view immediately after the browser completes the process of page construction. This is how “search engine optimization” (SEO) was born (Evans, 2007). Initially, it involved the web development activities necessary to, on the one hand, include keywords of interest in specific elements such as metatags, page titles and headlines and, on the other, embed links to pages with content on topics relevant to the outgoing link’s page. However, for the sake of keeping their websites among the top results, many webpage owners resorted to deceiving Google’s page ranking algorithm by applying abusive SEO tactics. Google realized that the widespread use of these techniques was hindering its primary goal of continuously delivering increasingly relevant lists of search results, that is, their distinctive value proposition.

Google responded by enhancing its page ranking algorithm, designing new intermediate variables to the process of sorting search results. Today, there are over two hundred of them (Dean, 2018). The one that I believe is of particular importance to my research is the “authority ranking” score, which Google patented with the title, “Search result ranking based on trust” (Guha, 1993b).This is a weighable variable that Google began utilizing in order to reward websites’ efforts to provide the design and information conditions necessary to deliver relevant, engaging and useful content consumption experiences to users. At its core, it is essentially an expression of a website’s semantic value vis-à-vis the keyword set that triggers its listing on Google’s search results’ page; a qualification that measures the extent to which a website embodies the necessary semantic elements to convey a given meaning or set of meanings. Although back in the late 90s, the algorithms evaluating these points of congruence relied mostly in keyword-based comparisons between the websites’ indexed content and post-search patterns of user-content interaction, today, advances

in artificial intelligence have steered algorithms' logic to focus on a more holistic understanding of user intent.[5]

Once the "authority" variable was brought to bear, websites would only rank well for the topics that prompted visitors to show behavioral signs indicating satisfactory user experiences. For instance, if a user landed on a website that was purportedly "about" topic "X" as a result of searching for topic "X," yet exited right after landing, Google may have registered the event as a potential sign indicating that the website did not provide a relevant experience vis-à-vis topic "X." Should this type of event become a trend for this particular website, Google could assign a low authority ranking score to the website. Thereafter, every time a user submitted a search query referring to topic "X," the website would either rank low on the list of research results or be excluded from it altogether.

Just as compounded poor user experiences could lead to low authority ranking scores, repeated interactions displaying behavioral signs of user satisfaction could lead to both high authority ranking scores and a continuous presence among the list's top results. Furthermore, since the first five results in Google's list account for roughly 74% of all clicks (Caphyon, 2019), high ranking websites tend to get more chances to reinforce their high authority ranking scores as well. Therefore, it follows that, for any given topic "X" that is searched for on Google.com, the first three to five information sources listed will tend to have a decisive role in its definition, not just because they tend to be the listing that users click on the most after performing a search, but also because the websites listed in these positions tend to maintain their top rankings regardless of the user that may be performing the search; a subject which I shall return to in chapter 3. Thus, in cultural contexts in which search engines are used as safe platforms to become acquainted with the unknowns of the physical world, Google's ranking algorithms have the effect of granting immense power to the first five information sources, whose claims, true or not, will tend to be regarded as knowledge on whatever particular subject the search query that triggered their listings was about.

Yet the search results that users view on Google are also influenced by factors exogenous to both the search engine and the company's ample repertoire of app channels. As mentioned before, the Semantic Web's Resource Description Framework

[5] The availability of unstructured, user-generated data has been equally critical to these advances in user profiling and intent forecasting.

(RDF) provided a series of new methods for the acquisition, processing and sharing of user-based information across website, application and community boundaries. This enabled Google to develop the informational mechanisms it needed to deliver increasingly individualized user experiences in which content "relevance" was defined according to a wider array of data points. These included age, gender, parenthood state, geographic location, browser language preference, type of device, operating system, search engine history and browsing history. Thus, in its quest to enhance the degree of relevance of user experiences, Google has managed to arrange both search results and ads that are relevant not only to the user as an individual, but also to the specific interests that define the individual at a particular moment in time (Guha, 1993a). Due to the great reach of its content network, Google is able to gather information from roughly 90% of the entire web. Furthermore, it is also able to establish similarities between and among users; a capability that it leverages with the intention of introducing interests that, while current to a cohort of individuals, may be just latent—or hitherto inexistent—in others that are otherwise "similar" to the cohort (Google, 2019a; b). When successful, this content management function can have the effect of forming massive, uniform, interest-based segments. Due to the effect that the authority ranking score mechanism has on the sorting of search results, these segments can also fall prey to the preconditioning of their points of view. It is now clear that the stark inter-group discrepancies that the U.S. experienced in the months leading up to election day were the product of the large-scale application of this type of clustering, opinion-making, information-arranging mechanisms (Electome, 2016; Vosoughi, Vijayarghavan*, et al.*, 2016; Gillani *et al.*, 2018; Kearney, 2019).

Since every time that a user visits a website is a new opportunity for its content to be shared on social networks such as Facebook and/or Twitter, a website listed at the top of Google's search results has greater chances of getting its content to be shared and reshared at exponential rates. Moreover, since the accumulation of visits indicating satisfactory information interactions leads to higher authority ranking scores, websites whose content becomes viral also have greater chances of remaining within the top positions of the list of search results. This search-engine-social-network traffic synergy can further exacerbate the forming of opinion clusters. Therefore, the same digital tools that users could utilize to engage in communicative action—the type of intersubjective process capable of exposing empirical inconsistencies in public

discourse—become instruments in the Establishment of a symbiotic relationship between intragroup belief reinforcement and concomitant intergroup alienation.

The scope and effectiveness of these alienating processes is amplified by a constant torrent of content production manifesting and feeding the process of online discursive construction. The relentlessness of this flow is directly related to a communicational pervasiveness that would be impossible, had web access remained restricted to the moments and spaces in which ethernet-wired desktop or laptop computers were available, for it is the readiness of portable devices capable of producing and wirelessly broadcasting datafied messages that maintains the torrent's constant flow filled with user-based, contextually-current content. This is the essence of the "mobile web;" a frontier in the expansion of cyberspace reached during the second half of the 2000s. Heralded by the rise of the slate-form, touchscreen smartphone, it is a paradigm that emerged through the convergence of powerful telecommunication and computing miniature instruments (i.e., nanotechnologies); highly simplified and robust, haptic GUIs; the datafication of telephone signals; the consolidation of data's function as a propeller of communicational processes between and among humans and machines; and the heightened socialization of data capturing, sharing and usage processes. The convergence of these phenomena can be witnessed in the socio-computational services that leverage both the miniature sizes and powerful processing capabilities of nanotechnologies towards the enhancement of human performance. These enhancements usually occur through the measurement and datafication of previously "invisible" or unquantifiable microtrends emerging from humans' and machines' execution of activities at all spheres and levels. More specifically, mobile ICTs abstract facts from the sensing and measurement of signals grasped from the physical world, which they transform into data that can be furthered processed for the presentation of information to either or both humans and machines. This information consumption derives human and artificial intelligence which can then be instrumentalized towards the improvement of activity performance. For instance, the machine-driven, decision-making assistance event that takes place when Google puts together the visual elements that make up its search results' pages and page-margin ads, or when Facebook selects what posts to present on a user's "newsfeed," is the result of an orchestrated, dynamic user experience construction process that aims to provide enhancements to humans' capacity to find information that is relevant to their individual, current contexts. And since nanotechnologies and datafication have

been embedded in the communicational processes that drive social, economic and political life at all levels, machines are fed plenty data points with which to construct users' and groups' "relevance" profiles in real-time.

Thanks to the inverse relationship between microprocessor's size, capacity and cost explained at the beginning of this section, online computing has spread to social contexts where computer-literacy and financial constraints had prevented it from becoming incorporated into daily-life. This englobes both individual and collective activities that previously could only be carried out on personal computers (e.g., checking email, reading status updates on Facebook's "newsfeed," etc.), that had never been conceived as "computable" or "computational" (e.g., getting a cab, automating the organization of workout routines based on a watch's "knowledge" of the bodybuilder's performance, planning a driving route based on real-time traffic statistics, etc.), or that were altogether inexistent prior to the rise of ubiquitous computing (twitting, snapchatting, facetiming, sexting, etc.). To be sure, while the perceived advantages of using these types of socio-computational services has played a major role in the depth and scope of mobile web's societal penetration, ICTs' ubiquity would be greatly diminished if people had to purchase the right to use them with some form of currency. However, most of them allow for partial or complete use of their service platforms in exchange for nothing more than users' personal data; most people appear to deem this exchange of knowledge for services a bargain, hence their popularity across all social strata. Nevertheless, when contextualized with cross-referenced data pin-pointing facts such as date, time, location, language, gender and age, together with all the ubiquitous facts learned through service usage, this personal information becomes the missing piece in the puzzle for the algorithms that evaluate user-oriented, conditions of relevance. Without this rich, dynamic, web flow of information and the data format standards with which to share it across application and domain boundaries, machines would not be able to grasp the nuances within the overarching societal trends observed in web searches. Thus, it is no exaggeration to say that the introduction of instruments capable of performing artificial-intelligence tasks to assist the most specific and individual activities is a major factor enabling the potential influencing of individuals' psyche—the prime condition for the execution of a successful massive social hack.

When it comes to the trajectory of cyberspace and how cyber-psycho-cognitive operations are intimately linked to its structural driving forces, there are certainly other

transcendental events and inventions worthy of a much longer discussion. However, it is not my intent to turn this analytical exercise into the context where such endeavor should take place. In final analysis, I believe that the roots of the “problematique” lie in the socioeconomic and technological conditions that make the expedient, widespread and profitable consumption and reproduction of alienating political narratives possible, the structural causes of which have been assessed in a chiefly chronological order: the affordability of ever-more-powerful and smaller computational devices, the socialization of computers, the successful simplification of complex information production and management tasks through GUIs, the preconditioning and uniformization of viewpoints through information architecture metaphors that seamlessly discourage critical thinking, the commoditization of online user experiences and the omnipresent financial and logistical backing of the American military apparatus and its associated scientific institutions.

3. THE STRUCTURE OF CYBER-PSYCHO-COGNITIVE OPERATIONS

Cyber-psycho-cognitive operations are complex political instruments designed and orchestrated to precipitate specific accelerated changes in sociopolitical behavior on a large scale through the management of people's online experiences. Data is their single most critical resource, for it informs the machine-learning processes guiding the automated configuration and execution of message construction and targeting strategies aimed to evoke specific emotions and behaviors in the audience. From extraction and appropriation to weaponized usage, cyber-psycho-cognitive operations' data lifecycle involves five actors: the data acquirers and generators, the mass media, the State, the political parties, and the users who consume content and produce data through their interactions with content; the prosumers.[6]

Although their rationales differ, the first four actors exercise regimes of what Weber called "administrative secrecy" vis-à-vis the types of data that can be extracted and appropriated from the users; bureaucratic mechanisms employed to hide their knowledge, action and intentions from the public in order to avoid scrutiny and criticism (Weber, 1978, p. 992). Whereas users relinquish any form of control over their own privacy by accepting the data acquirer's and generators' platform usage policies, the bureaucracies of the cyber-psycho-cognitive operations' leading actors are rendered opaque from all angles as they gravitate around the utilization of users' data in a multipolar relationship that fluctuates from partnership to animosity. Yet, as it is common practice in regimes of administrative secrecy, this opacity is maintained under the disguise of transparency through discursive construction practices. Cyber-psycho-cognitive operations are propelled by both what is kept from and what is constructed for public view. Each actor plays a part in the *problematique*.

[6] This composition is based on the events leading up to the American presidential election of 2016.

3.1. POLITICAL ACTORS

3.1.1. Prosumers

ICTs and the socioeconomic and communicational practices that they propagated across the globe turned data into the primary commodity of the current mode of production (Castells, 2010b; Bean, 2017). Yet the value of data lies not in the digital objects themselves. Rather, it lies in the fact that, without having to go through destructive transformational processes, it can produce the information necessary to maximize the productivity and efficiency of other production processes (Hammond, 2013; Monino, 2016). Moreover, insofar as the data refers to variables that are relevant to the target production process, it can be recombined and repurposed to produce further information, thus generating “cycles of continuous improvement.”

With the rise of technologies such as search engines and social networks, web service companies became capable of not only tracking, but also decoding the meaning and, eventually, the intent behind ICT user-information interactions (Gatti *et al.*, 2014; Törnberg and Törnberg, 2018). The advent of the Semantic Web enabled services to normalize the codification of this semantically-enriched metadata in a way in which it could be shared beyond platforms’ limits and hence, inform the construction of user-oriented navigation experiences across their virtual walls (Ahmadi *et al.*, 2016). Later, the “big bang” of mobile web technologies added even more types of data points, which referred to real-life scenarios that were previously inaccessible due to the logistic constraints imposed by the size and weight of computers.

More recently, the Internet of Things (IoT) has taken ubiquity to the next level by adding Artificial Intelligence capabilities to pre-ICT-revolution machines, appliances and other kinds of everyday-life artefacts. These AI-powered machines will “know” how to drive people home, how they like their clothes washed, how hot their coffee should be and just how brown they want their toasts every morning. But they will not keep it a secret because every little detail is a way in which each person is different from another and similar to a few thousand more (Barbu, 2014; Shmueli, 2017). And calculating how each of these segments can be more or less profitable vis-à-vis market “X” or “Y” is precisely how the enrichment of data through user interactions does in fact translate into data’s economic value increases (Ramer *et al.*, 2009a; b; Perler, 2013).

Thus, it began as—and may always feel like—a game: playing with interfaces that somehow "knew" one's intent. They were always one step ahead. If someone searched for the word, "jeans" in Google, the person would see concept-related ads during the following "X" number of days. And they would "print" not only on Google.com; they would essentially permeate entire web navigation sessions, including news blogs, directories, dictionary pages, retailer websites and social media. The idea was to deliver increasingly personalized, contextually-relevant content to each user. From a data-commoditization perspective, what this meant was that, after accepting websites' cookie policies, users' "free" interactions with content would be acknowledged and enriched with all the qualifiers describing the contexts in which they happened.

Today, these compounded meta-information packages provide a critical part of the information that Internet advertising platforms "rent" to advertisers seeking to reach not just the person who searched for the word "jeans," but also all the people that may be similar in one or more aspects; from traditional demographics to specific behavioral patterns. The person who was simply looking for "jeans" in what he or she believed was a free search engine. Little did she know that the act itself was generating profit for the search engine owners. In general terms, this is digital prosumerism (Ritzer and Jurgenson, 2010). The kind that applies to cyber-psycho-cognitive operations shares the mechanics of the example but is not nearly as benign. This will be discussed in further detail when I explain the machine-driven mechanisms that condition users' processes of knowledge construction through principles of authority and relevance.

For now, suffice to say that human-information interactions express, reinforce and feed the knowledge structure of power by legitimizing the human-made and machine-driven mechanisms regulating the construction of informational experiences. It is through these informational, experiential processes that individuals share symbols and construct meanings among themselves, interweaving a virtual spatiotemporal context in which ideas are formulated, socialized and used as if they were "knowledge" and "information;" even if they have not been subjected to rigorous scientific validation. This is how "fake" and "real" news spread throughout the Internet and the logic of profitability—not just free speech—is what makes them circulate sometimes hand-in-hand.

3.1.2. Data Acquirers and Generators

Google, Facebook, Microsoft, Twitter, Apple, Amazon, Uber, Netflix, IBM, Experian; the list is much longer, and it even includes companies dedicated to activities whose direct relationship to user-generated data is anything but traditional (e.g., fashion design, farming, dining, lodging, to name a few) (Marr, 2016; Mazzeia and Noble, 2017). As do the other three actors involved in the orchestration of cyber-psycho-cognitive operations, the data acquirers and generators seek to strengthen their positions in the power struggle at the prosumers' and the other actors' expense (Bolin and Schwarz, 2015; Ritzer, 2015). In exchange for "free" content and web social services, the data acquirers and generators reap users of the data they produce through a "customer journey" of content interactions (Cooley *et al.*, 1997), weaving a dynamic web of interest-, preference- and affinity-based relationships between and among users, persona archetypes and semantic and syntactic entities (Ramer *et al.*, 2009a; Najjar and Kettinger, 2013). Machine-learning algorithms capabilities allow them to refine these audiences utilizing Natural Language Processing methods in order to grasp linguistic nuances from published text (Chen *et al.*, 2011). This enables them to make inferences about both the phrases' semantic and sentimental contexts and, as sentiments are expressions of a person's psychological state (Liu, 2015), they can use their intelligence to tailor and micro-target messages guided by communicational strategies geared toward the fulfilment of goals revolving around the effective change of specific behavioral patterns (Cao *et al.*, 2014).

Furthermore, these systems are reactive; they try message configurations that have worked in the past with users of similar characteristics and, if they do not get the expected results, they learn and try a different message configuration the next time around (Begeja *et al.*, 2008; Toms *et al.*, 2008; Vijayaraghavan *et al.*, 2014; Zimmerman *et al.*, 2014; Vicioso, 2015a; b; Aggarwal *et al.*, 2016; Zamanzadeh *et al.*, 2018). Moreover, they can afford to be persistent because their dynamic reactions are based on signals sent from the entire family of devices and channels users have ongoing sessions (Manolarakis *et al.*, 2014; Katz *et al.*, 2016). Therefore, the data they base their messages on is contextually relevant in demographic, spatiotemporal and psychological terms; all thanks to the pervasiveness and ubiquity of the personal devices and social profiles that are constantly sending signals back to these machine-learning systems (Lewis *et al.*, 2009; Barbu, 2014). Every selfie posted from a mass

demonstration, every live video uploaded from a torch-lit rally, every heated, electronic-forum argument with a "troll," or any other type of politically-charged, behavioral manifestation in which a user may engage online is a new combination of semantic sentiment metadata signal being sent to the machines(Halpin, 2013; Rosenthal *et al.*, 2014; Yan *et al.*, 2015). It is essentially as if their "gaze [was] alert everywhere" (Foucault, 1995, p. 195).

The degree of specificity and precision with which machine-learning algorithms can approximate a person's current interests and conditions increases the potential gains of accessing their intelligence, making data increasingly valuable to all the other actors in the struggle (Sadowski, 2019). One of the main reasons for this is because it serves as computational input in the decision-making process of assigning data-driven tags to categorize the signal sender as a persona at a particular point in a path towards the fulfilment of a desired goal—a path calculated by statistical probability (Simmons and Catanzaro, 2012; Vázquez *et al.*, 2014; Zimmerman *et al.*, 2014; Chang and Kannan, 2015). This goal can be personal; the person can be trying to find information about political candidates' platforms, trying to decide what movie to watch next weekend, or if getting a life insurance is a good idea. But machine-learning systems turn all the actions the user performs in the process towards the achievement of this goal into data that can help the other actors in the operation achieve their goals "at the person's expense" (e.g., web analytics algorithms study user-information behavior at a given location and conclude that roughly 75% of the town is going bankrupt. A moneylender happens to be running an automated advertising campaign at the time. The two systems will "talk" and this will result in the advertising engine configuring ads with creative assets that it "thinks" will yield leads for the moneylender).[7] And, provided they have been configured to extract, store and interpret the user's data adequately, sentiment-aware neural networks can maximize both the efficiency and effectiveness

[7] The machine-learning algorithms will receive all the metadata and semantic signals produced through user-content interactions and provide it to the political candidate, the cinema or the insurance company as information that can be used as input in a variety of other intelligent systems. One of the main objectives of this machine-assisted, decision-making process is to identify whether the person should be included or excluded from the paid communication efforts, and how near or how far the person is to achieve the client's desired action. The potentially multi-session, multi-device, multi-channel, multi-campaign user-data interaction path towards the fulfilment of a desired action is what in digital marketing is typically called "a conversion funnel." Marketers' mission used to end when "desired actions" where fulfilled on specific digital properties (i.e., websites, apps, etc.), but now, even storefront, in-person purchases can be tracked as "digital conversions." What is preventing their clients from applying this concept to voting booths? Certainly, the technical side of the problem has been taken care of.

with which such goal-achievement process is conducted through semi- and fully-automated workflows.

How this works to the advantage of the systems' owners is no secret; the digital marketing platforms expect their specialists to know this type of information before they take their certification renewal exams every year (Google, 2019d). Neural networks interpret a given number of data signals from thousands of user sessions on a given context of interest (i.e., a website, a segment, machine-defined audience, etc.), identify the ones that have been most successful vis-à-vis a given client goal and derive user data patterns to characterize the personas behind these sessions (Google, 2019e). Then, choosing assets from a content inventory created by marketing specialists, advertising AI-powered machines construct user-oriented ads based on what they "think" will generate the intended responses from the audience cohorts. This "thinking" process is the calculation of a probability that takes into consideration statistical data obtained from thousands of user sessions with similar values for a definite set of variables. Combining and recombining assets one ad impression after another, advertising machines perform continuous trial-and-error exercises, registering their experiments and their results, constantly optimizing according to a set of client-configured priorities. This is how they find the best-performing ad configurations.

Since the monetizable event for the advertising platforms is the user click, this is the event they want to have the machines facilitate the most possible. Through a never-ending sequence of successes and failures, machines learn how to accomplish this in such a way that it also maximizes advertisers' desired goals (i.e., turning users who did not click on ads into users who clicked on at least one ad and performed the client's desired action in the digital context hosting the product or service being promoted). In this process, data inventories are also improved through semantic enrichment and frequent validation, thereby increasing the perceived value of both the data acquirers' and generators' service and their data. This is in general terms the logic that propels these companies; like any other company, they pursue profit-making. Their administrative secrecy (Weber, 1978, p. 992) seems to be circumscribed to this logic as well.

3.1.3. The Mass Media

The mass media are in charge of creating the illusion of transparency that keeps the public from realizing the real opacity of the operation they are a part of. TV and radio networks, newspapers, magazines and their online channels; they all serve as discursive stages for company, party or government representatives to provide statements that they wish to deliver as "facts about real facts" that cannot be shown directly for one reason or another. They deliver believable performances of their intended roles—from spatial context for message delivery, to dress code, vocabulary, articulation and demeanor. The public—apathetic to the media's role in the process of knowledge construction—follows suit; unconsciously confers the representative the power to grant "knowledge status" to the statements delivered on stage. A prime example of this was given the day that Hillary Clinton's campaign started the cyber-psycho-cognitive operation that would eventually lead to then-President Barack Obama's state of emergency declaration on December 29, 2016:

> Jake Tapper:[8] What is the reaction of the Clinton campaign to these DNC, leaked emails suggesting that top officials, including the CFO there, were actively discussing ways to hurt Bernie Sanders in the primaries?
>
> Robby Mook:[9] Well, I think the DNC needs to look into this and take appropriate action and I'm sure that they will.[10] What's disturbing to us is that we, uh[11]...*experts are telling us* that, uh, *Russian State actors* broke into the DNC, stole these emails, and, uh, *other experts are now saying that the Russians are releasing these emails for the purpose of actually helping Donald Trump* (…) I think we need to be concerned that (…) Trump and his allies made changes to the Republican platform to make it more pro-Russian (…) So, I think when you put all of this together is a disturbing picture and I think voters need to reflect on that.

---

[8] Chief Washington Correspondent for CNN, who, to be fair, did ask questions that pressured Mook to go from a discourse of certainty to one of doubt. Unfortunately, regardless of the ethics and professionalism which may characterize the work of specific journalists in mainstream media, this does not change the fact that the type of institutions they work for serve, first and foremost, the interests of private groups.

[9] Hillary Clinton's former campaign manager.

[10] Pay attention to how Mook essentially dismisses Tapper's question and sets a totally different agenda for the rest of the interview.

[11] I transcribed Mook's utterances of uncertainty to show the precise moments when he is unable to hide his lack of confidence in what he is about to state next. Notice that in most cases it is some type of reference an off-the-scene collective abstract figure; either "the Russians" or the so-called "experts." The latter's "existence" is extremely convenient: they take all the credit for the "findings" that Mook is sharing with the audience. They are "experts," therefore, "they really know what they are talking about," but, if their "findings" happen to be incorrect, it is not Mook's fault. For the next few months, the so-called "experts" were mentioned time and again by many other DNC representatives. None of the mentioned "experts" would ever show up in front of a camera to explain in detail just how exactly it was that the true nationality and location of the person or people behind "the break-in" were determined.

> Jake Tapper: What evidence is there that the Russians were behind this in terms of the hacking, or in terms of the timing by WikiLeaks?
>
> Robby Mook: Well, I, I... *we need to let the experts speak on this*. It's been reported on in the press[12] that the hackers that got into the DNC are very likely to be, uh, working in coordination, uh, with Russia. And again, I think it's..if the Russians in fact had these emails, again, I don't think is very coincidental that they're being released at this time to..to create maximum damage on Hillary Clinton and *to help Donald Trump*.
>
> Jake Tapper: But it's a very, very strong charge that you're leveling here. You're basically suggesting that Russians hacked into the DNC and now are releasing these files through WikiLeaks to help elect Donald Trump.
>
> Robby Mook: Well, *this isn't my assertion. There are a number of experts* that are asserting this. I think that we need to get to the bottom of *these facts* but *that is what experts are telling us*. *Experts have said* that it is the Russians that *in fact* went in and took these emails and, and, then, then, if, if, if they are the ones who took them, then we are to infer that then they are the ones that are releasing them (Mook, 2016).

The stage Mook and Tapper were having their interview on was surrounded by a few hundred million windows from all over the U.S. and the rest of the world; is there anything opaque about this? It seems as transparent as it can possibly get: a head-and-shoulder-shot of a sharp-looking young man, with a “campaign manager” caption right next to his full name, using a lexicon that seems to match the title and—of critical importance—appearing on one of the main news channels being interviewed by no other than one of the channels’ personalities of all time. The construct has all the discursive signs that signal trustworthiness to viewers, therefore, they remember whatever these two performers discuss as “facts.” The seriousness of these “facts” was summarized by Tapper’s reaction: “it's a very, very strong charge that you're leveling here. You're basically suggesting that Russians hacked into the DNC and now are releasing these files through WikiLeaks to help elect Donald Trump.” This is the kind of “news” that tends to go viral in seconds. By the time the interview was online on some shareable format the problem was twofold: the veracity of the “facts” had not been properly established and, in spite of that, CNN’s report was perceived as an exclusive, which not only kept viewers sharing and resharing their content, but also made CNN’s competitors look for “news” of their own. Needless to say, this accelerated the speed with which rumor became “fact” and sparked the kinds of fears, speculations

[12] Per Tapper’s later comment referring to the gravity of Mook’s accusations, it can be inferred that the interviewee was in fact “breaking the news” of the alleged Russian-Trump collusion to CNN’s nationwide audience. I tried to find earlier records of the claim and could not find any. Therefore, this interview seems to be the event that set Clinton’s cyber psycho-cognitive operation in motion.

and heated discussions that a factual collusion between a presidential candidate and one of the country's main military and political rivals would spark.

Before the ICT revolution put in everyone's hands the instruments to partake of the nonstop debate, at least mainstream media would not have the digital monetization incentive to go with the flow. But more clicks on video links lead to more page landings, which lead to more ad impressions, which lead to more clicks and more advertising revenue. Suddenly, the rumor pays off more than the story about, "who are Mook's so-called experts and where can we find them?" Hunting such story would have entailed drilling into the Democratic Party's administrative secrecy, getting their "experts" on the record explaining everything; from their methodologies, methods and findings, to how they acquired such expertise. Eventually, this line of questioning would have probably gone back to Mook's statements, which would have then been revaluated under the light of public—perhaps even scientific—scrutiny. This how this cyber-psycho-cognitive operation could have probably been brought to a halt: going beyond the representative's statements to verify first-hand whether what he referred to as "facts" even existed. But instead, this turned out to be an example of how the process of driving the cyber-psycho-cognitive operation forward is a process of maintaining and reinforcing its opacity through semblances of transparency.

Using these seemingly "accredited," "knowledgeable," "credible," "insider" individuals as "gatekeepers," political parties, companies and government institutions feed the public whatever (mis)information seems instrumental to keep their secrets guarded while projecting "the illusion of transparency." This "public relations façade" allows them to move forward in the pursuit of their power interests. Mainstream media's role is to provide the scenarios where these dramatizations can be legitimized as "facts" ready to become "public knowledge." Thus, they piece together stories as audiovisual collages of statements from national and foreign state officials, government agency spokespeople, political candidates, IT security experts and even military strategists. Their declarations are framed as utterances referring not to beliefs and suspicions, but to "the fact of the matter;" stories about "evidence" that stand in the place of the evidence itself in the public process of knowledge construction.

Though the rise of ICTs has led to the instant mediatization of representatives' "knowledge" dramatizations, the notion of knowledge as a discursive product emanating from the authority figure of the "expert bureaucrat" is at least as old as Weber's theory of bureaucracy (Weber, 1978). Nevertheless, the immediate

mediatization is, however, a critical differential factor in the success of the cyber-psycho-cognitive operation, for it reduces the window of opportunity there is to challenge the veracity of information that is being communicated in front the audience. From a methodological perspective this, too, should be taken into account, for if immediacy and speed are mission-critical to the operation's success, then in vitro research methods unable to reliably register the subjective factors involved in the spread of (mis)information—sentiments as individual expressions of psychological states, for instance—should not be counted on when studying cyber-psycho-cognitive operations.

3.1.4. Political Parties

From a discursive point of view, political parties' battle is as much about visibility and attention as it is about self-definition. This means not only defining themselves coherently before the audience, but also having their own definitions prevail over the definitions that rivals will try to supplant them with in the minds of the voters. This is particularly true during decisive moments such as electoral periods, in which party candidates tend to emphasize what differentiates them from the other options on the ballot. These missions turn political parties into immediate clients for both mainstream media and digital advertising platforms. From the first, they rent stages, pundits, stories and, of course, channels from the first. From the latter, they get the video time and screen real-estate needed to make all the content created in their favor visible to the audiences that can count the most on election day. So far, this reads like regular electoral party politics.

Nevertheless, this changes in a context in which information access is increasingly mediated by personalized, data-driven, machine recommendations, which was exactly the context in which the American presidential election of 2016 took place. Programmed with the logic to create the conditions for people to have "end-to-end, relevant, online experiences," machine-learning systems tend to push all kinds of "relevant content" towards users' field of view; from web pages, to social profiles, service and product ads, sponsored comments, events, tweets and more. Similarity between and among pieces of content leads to hours on end of consuming self-reinforcing ideas about the physical world. Moreover, as profiles, forums and events are also included in the potential types of machine-recommended items a user may

“stumble upon” while navigating online, the likelihood of engaging in communicative action with similar peers increases. Developing a sense of belongingness through loose or informal political party affiliation further raises the probability. In November 2016, all these psychosocial communicational factors were at play as instruments in the construction of polarizing discourse. Emanating from inherently polarizing candidates, campaigning on a socially polarized nation, the result of their application was the creation of one of the most socio-politically divided, electoral scenarios that the U.S. has ever witnessed. Essentially, it could be described as two separate groups living the same objective conditions while experiencing diametrically opposite intersubjective realities.

Thinking in abstract terms, I would argue that the dangers that may come as a result of this type of division are proportional to the orientation of the divisive discourse spread within the “digital echo chambers” and its resonance in the audience communities. Furthermore, I would also argue that, as machine-learning systems offer the advantage of automating message targeting and configuration based on sentimental semantics, candidates whose discursive end goals are more intimately linked to the evocation of specific feelings and emotions in their audiences will find in the use of these systems a greater strategic advantage on the ground than those with less sentiment-dependent discursive end goals. Therefore, if a candidate’s self-definition/differentiation strategy is based on a type of divisive discourse based on sentimental semantics, the speed, precision and persistence of machine-learning systems will likely amplify the candidate’s advantage over his or her rivals. By the same token, the dangers that such discourse may bring to the social fabric are proportional to the degree of relevance between the messages delivered by the machine-learning systems and the targeted areas’ pressing issues. From the point of view of AI-powered, marketing and communication systems, these reflections may lay the groundwork for an explanation as to why Donald Trump won the discursive battles in the precincts that he needed to secure the presidency. But more important to this discussion, these are the principles that explain the difference between Clinton’s and Trump’s two cyber-psycho-cognitive operations: the single “preemptive legitimacy crisis” vs. the “preemptive legitimacy crisis” with a parallel securitization move approach.

Jürgen Habermas’ observations regarding “the relation of legitimacy to truth” in Max Weber’s concept of rational authority provide a useful lens to understand the type of legitimacy crisis that both Clinton and Trump prepared for each other:

> If belief in legitimacy is conceived as an empirical phenomenon without an immanent relation to truth, the grounds upon which it is explicitly based have only psychological significance. Whether such grounds can sufficiently stabilize a given belief in legitimacy depends on the institutionalized prejudices and observable behavioral dispositions of the group in question (Habermas, 1992, p. 97).

The only claim to legitimate authority that presidential candidates have while campaigning is their presidentiality potential. In other words, the fact that they "meet the institutionalized prejudices and observable behavioral dispositions" of, in this case, the American people. In this sense, as Habermas observes, it is purely psychological. Thus, by making an immediately mediatized claimed such as, "experts are now saying that the Russians are releasing [the Podesta] emails for the purpose of actually helping Donald Trump," Clinton's campaign manager, Robbie Mook, appealed to Americans' Cold-War-rooted, institutionalized prejudice against Russians in an attempt to hinder the nation's ability to legitimize him as president. His strategy was to frame Trump as a "traitor" who, as such, could not embody what would be the "system-imperative" (Habermas, 1992, p. 2) qualities of "an American president"—deeply imbued in notions of "nationalism" and "patriotism." In these terms, electing him was the equivalent of introducing structural incompatibilities into the system; a legitimacy crisis.

This is precisely the type of political strike that a "preemptive legitimacy crisis" can deliver: a presidential term that begins shrouded in doubt, suspicion and mistrust. A president in such scenario is likely to start with limited public support and still see it decay for the following years if allegations are not put to rest—as they have not. Trump's victory notwithstanding, the office of the presidency is structurally tied to a "truth-independent" notion of legitimacy; the legality of holding public office does not shield the president from the political effects that may unravel from the impact that a successful framing as a "traitor" may have on the American psyche. Thus, it comes as no surprise that this is a formal investigation that the Democrats have invested millions of taxpayer dollars in maintaining over the past two years—and their investment may still yield the returns they have longed for. Theoretically, even now that the findings laid out in Special Counsel Robert Mueller's investigation report have been officially constructed as a statement of lack of evidence to prove collusion between "Russian state actors" and Trump, this information could still suffice to generate the psychological effects needed to open articles of impeachment. In fact, in the wake of the release of the report's summary, the Democrats began to cast doubt in the

investigation, its findings and the alleged dubious political interests behind the redaction and publication process. Would they be doing the same if the summary had been tailored to their political needs?

Political authority in the U.S. is particularly susceptible to the threat of cyber-psycho-cognitive operations because legitimacy seems to remain circumscribed to its psychological dimension. Even after presidents are sworn into office, people's perception of the validity of their claim to legitimate authority is tacitly strengthened or diminished based on an ongoing comparison between their perceptions of the president and the archetype of "the one with a right to legitimate authority." Therefore, rendering the public's perception of a presidential candidate unfit to match such archetype would insert a psychological constraint that would inhibit the electorate to vote for him or her. Campaign manager Mook tried to do this by mediatizing a political narrative. On the other hand, the Trump campaign and parties working on its behalf managed to do this more effectively by releasing thousands of compromising emails that were sent or received by Clinton and other close campaign and party collaborators. The content of the emails multiplied in a slew of articles, tweets, posts, memes and videos, creating a latent aura of "unpresidentiality" that would accompany Clinton for most of the campaign trail. Thus, what on paper seemed like an outstanding curriculum vitae for a president was tarnished by thousands of pieces of back-and-forth correspondence with many known politicians and personalities. Among the issues discussed in many of these exchanges were secret quid pro quo agreements that amounted to grave acts of corruption involving Clinton, her husband, their foundation, the State Department and the DNC. This, coupled with what Jake Tapper alluded to in his first question to Robbie Mook (i.e., "What is the reaction of the Clinton campaign to these DNC, leaked emails suggesting that top officials, including the CFO there, were actively discussing ways to hurt Bernie Sanders in the primaries?") drove the two voting trends that would seal Clinton's final demise: voters in key "blue" precincts switching sides and Democrats abstaining, presumably disillusioned with their candidate's character.

Turning a candidate into "the archetype of a corrupt politician" in the eyes of the electorate may have sufficed to bury Clinton's—and even Trump's—chances of becoming president of the U.S. However, Trump's self-definition/differential strategy had constructed him as the only person capable of leading the American people in the face of existential threats. To millions of Americans, his "critical" role towards "the

nation's survival" made his character's flaws seemed "insignificant" or "negligible" by comparison. This was so because they were "enchanted" by the political narrative that permeated their digital echo chambers. "The national reality" constructed in this narrative was one where, "due to the irresponsible actions of the Washington Establishment," the nation had been left fully unprotected against the infiltration of "foreign elements" who were threatening the security of the nation and "the American way of life." According to Trump, the cultural and political origins of these "foreign elements" turned them "inherently incompatible." Accordingly, any integration attempt, whether it be the result of an American initiative or theirs, represented a structural danger to the system. This was, in fact, the main explanation for the current state of crisis in which the country was in; an introduction of structural contradictions of foreign origin: from foreign trade, to visas for high-skilled foreign workers. Add to this "migrant terrorists," "Mexican stealing jobs" and the need for a "big, beautiful wall" and you got a summary of what Trump's securitization discourse was about.

How was it weaponized? Machine-learning systems capable of processing natural language while continuously refining their detection and understanding of nuances in sentiment semantics. These sets of systematic routines constitute the most efficient and effective methods for the preparation of the psychological conditions under which groups of agents in a lifeworld are persuaded to redefine their psychosocial relations to other agents according to the political semantic value ascribed to them in the discourse of a securitizing political figure. In pre-ICT-revolution times, the securitizing agent used to signal the start of this process through the utterance of a speech act. Today, machine-learning microtargeted communication systems have perfected the execution of the process; nonresponders would be identified, categorized in segments and be bombarded with the right line, the right image, the right video, the right tweet, the right sponsored comment, the right article and so on, until they hear the starting shot. Then, they would join the rest in a spatiotemporal interval where the normal operation of the sociopolitical system has been suspended in one or more ways.

As Habermas points out, "crises in social systems are not produced through accidental changes in the environment, but through structurally inherent system-imperatives that are incompatible and cannot be hierarchically integrated" (Habermas, 1992, p. 2). Yet, as part of Nation-State projects, country elites manage and avert socio-systemic crises by institutionalizing political narratives that help civil society cope

with the incompatible system-imperatives that cannot be hierarchically integrated. The U.S. elites, for instance, supported the incorporation of the myth of “the melting pot” into mainstream American culture as a sociocultural mechanism to cope with the socioeconomic contradictions stemming from a history of structural violence and exploitation erected along ethno-racial lines. Nevertheless, despite the empirically verifiable elements of the myth of “the melting pot,” it is essentially discursive in nature.

Taking advantage of this, Trump introduced disruptive elements in the discursive environment, the first of which was the narrative of “a white America becoming a minority under threat by an avalanche of increasingly nonwhite people who claim or want to be American but could not possibly be.” Once the threatened “minority” had been discursively constructed, it was the turn of the threats themselves. Taking ethno-racial identity as the transversal security issue, he proceeded to securitize the influx of skilled and unskilled migrant workers, the internationalization of local manufacturing, the country’s free-trade agreements, and the naturalization and citizenship of the second- and third-generation immigrants. Having created all the narrative lines, it was time to feed them through communicative action both online and on the ground, this would bring about the rupture with normalcy he needed in order to make many voters see his platform as the only sensible agenda for the U.S. going forward, thereby obsoleting any other alternative.

Key to this objective is the mediatic representation and public perception of the spatiotemporal interval in the normal sociopolitical order. Its dramatization in the public sphere is intended to contain supportive elements in favor of the securitizing agent’s political narrative. Due to this, the suspension of the sociopolitical order itself cannot be discursively aleatory. The most effective way of ensuring its discursive alignment is having be the behavioral manifestation of the emotions arisen during the psychosocial exchanges occurring in the context of the contradictions discursively inserted in the lifeworld through the political semantic value ascribed to selected groups of agents. In other words, having the actions of agents on the ground serve as proof of the validity of the discourse’s main arguments—or what some would call, a self-fulfilled prophecy. In the case of the Trump campaign, the structural contradictions exploited to bring about the rupture with normalcy were essentially ethno-racial. This explains a type of chronological sequence that became common during his campaign’s trail: the announcement of a controversial initiative oriented to amplify ethno-racial segregation

and international isolationism, massive rallies mixing supporters and detractors turning violent, increase of media coverage, increase in popularity.

These behaviors arise from emotions and these are, in turn, products of psychological arousal. Therefore, one of the campaign's communicational goals must be to create the adequate psychological conditions for the evocation of specific emotions. The two emotions that are natural in a threat situation—even if it is only real as a narrative construct—are fear and anger, both of which provoke behaviors of strife. Strife, on the other hand, leaves traces beyond the public sphere, in formats that are machine-readable, especially when the communication medium of choice conditions the user to be spontaneous (e.g., Twitter). Furthermore, in this day and age, if a human expression is "machine-readable," it is also contextualizable in the larger realm of sentiment semantics provided by online public discourse. This means that the user can be categorized as being part of a segment and scheduled for the reception of machine-configured, micro-targeted messages. Provided that the marketing asset repositories have been adequately configured, AI-powered communication engine should be able to treat the user as if he or she were a magnet of all the content elements necessary to get to the stage of fear and anger where his or her communicative actions are dramatized in alignment with the securitization act's political narrative. At this point, every dramatization of fear and anger seem to get the securitizing actor one step closer to achieving the final confirmation needed. Thereafter, applying the envisioned extraordinary measures to solve previously inexistent problems will be legitimate and justified. What may not be under control is the social polarization and strife unleashed to get there. This is precisely one of the dangerous scenarios that may be drawn out of the Pandora's box that comes with every cyber-psycho-cognitive operation.

3.1.5. The State

Even prior to receiving the final report from the investigation started at the behest of the DNC, a high-ranking, U.S. official of the stature of no less than vice-president Joe Biden confidently suggested that Russians were behind a smear campaign against Hillary Clinton on behalf of Donald Trump. In other words, a Democrat government official publicly supported the narrative that would harm the electability of the other party's candidate beyond repair, even though the narrative had not been proven factual. Furthermore, to show just how sure the government was

about “the Russian meddling in the elections,” he escalated the tone of the rhetoric to talk about “imminent retaliatory measures.” This was the point in which Hillary Clinton’s cyber-psycho-cognitive operation transcended the domestic arena and became an issue of international security. Diplomatic threat exchanges through media channels were followed by real sanctions and a declaration of state of emergency on December 29, 2016. On January 7, 2017 came out the intelligence report on which all following reports were to be based: The Intelligence Community Assessment (ICA).

Stamped with the seals of the Office of the Director of National Intelligence (ODNI) and compiling findings from the CIA, the NSA and the FBI, the report has two key disclaimers on its first page. The first one justifies the fact that the document will provide little to no supporting evidence for its conclusions, even though it exists somewhere:

> This report is a declassified version of a highly classified assessment. This document’s conclusions are identical to the highly classified assessment, but this document does not include the full supporting information, including specific intelligence on key elements of the influence campaign (Office of the Director of National Intelligence, 2017).

The second one creates an expectation of objectivity nonetheless:

> We did not make an assessment of the impact that Russian activities had on the outcome of the 2016 election. The US Intelligence Community is charged with monitoring and assessing the intentions, capabilities, and actions of foreign actors; it does not analyze US political processes or US public opinion.

This promise, however, was short-lived, for the assessed intentions had already become part and parcel of the U.S. political process months before the report came out:

> We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia’s goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments.
>
> We also assess Putin and the Russian Government aspired to help President-elect Trump’s election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

Albeit phrased in intelligence lexicon, the report essentially reads like campaign manager Roobie Mook’s declarations. One is almost inclined to reply quoting Tapper:

> What evidence is there that the Russians were behind this (…)? (…) it's a very, very strong charge that you're leveling here (…) that Russians hacked into the DNC (…) to help elect Donald Trump.

Unfortunately, Mook's "experts" would answer the question in a rather similar fashion; by alluding to the existence of a third element—always part of the narrative, yet never present—which is the one that "knows." In this case, it is the full report, which is "a highly classified assessment (…) including specific intelligence on key elements of the influence campaign." Yet, while providing no conclusive evidence to support the exact same claims as the ones that started the cyber-psycho-cognitive operation, the ICA has served as the basis for numerous other statements and reports from various State institutions and government branches, each legitimizing the last.

One ought to wonder, what was born first, Mook's instantly televised claim, or the intelligence community's findings? The fact that there is no way of knowing highlights precisely the main challenge of studying the State as an actor in a cyber-psycho-cognitive operation: the agencies and branches involved have the strictest regimes of administrative secrecy of the entire State apparatus. Therefore, they are the opaquest; whatever they release as evidence could very well be nothing more than an instrument to advance a hidden agenda and there is no way of telling which the case is, for no one is entitled to know the truth. They will seem to be transparent because historically the semblance of transparency has been part of the American government's culture, but at the end of the day, they are intelligence agencies; keeping State secrets is part of what they do. Therefore, I would argue that government agency investigation reports are unreliable sources for the scientific study of cyber-psycho-cognitive operations. This is valid for at least all research carried out outside of the intelligence agencies' "circle of trust;" the privilege scientists who could presumably corroborate first-hand whether the original reports exist and meet scientific research requirements. Nevertheless, out of all the actors involved in the cyber-psycho-cognitive operation, it is the State that has the prerogative to declare war. Studying how States define, detect, attribute and participate in cyber-psycho-cognitive operations is imperative, but expecting State officials to provide methodological explanations detailing these processes is most likely pointless. Therefore, I believe the only way to develop reliable knowledge of cyber-psycho-cognitive operations is through the direct analysis of online discourse.

3.2. PROCESSESUAL COMPONENTS

3.2.1. Production of ignorance through the mediatization of experiences of reality

The (im)media(te) mental processing of spatiotemporally-compressed, third-party constructs of "reality" as "knowledge" produces ignorance. And, insofar as it is reproduced through relations between actors or collectivities, and it is integrated as an organizing element of regular social practice, both ignorance and its production are structural to the system. Furthermore, the structural production of ignorance plays the role of a necessary, yet insufficient condition vis-à-vis the effectiveness of cyber-psycho-cognitive operations. Anthony Giddens' Theory of Structuration (Giddens, 1984) provided the foundational elements for these premises: individuals' agency is constraint by the "rules and resources" that are "organized as properties of a social system." When adopted as part of popular culture, ICTs' capabilities led to a generalized acceptance of the belief that the communicational outcomes of spacetime compression—a concept I borrowed from David Harvey (Harvey, 1991; 2003)—could be regarded as faithful representations of "what is actually happening in the other end." The belief became institutionalized as the rule that such communicational outcomes could be processed as "knowledge" and, since knowledge is informational society's main resource (Castells, 2010b), they also became a resource on par with empirically-verifiable, first-hand knowledge. Ignorance was a resource in this process insofar as it generated the psycho-cognitive conditions under which messages' instantaneousness and immediacy could be interpreted as signs of "accuracy," "truthfulness" and "verifiability," all of them properties that are socially associated with the notion of "information" (Sloman and Fernbach, 2017). Constant individual repetition and collective generalization of this psycho-cognitive behavior led to the formation of a series of associated beliefs and social practices (Gunther; Adoni and Mane, 1984; Oreskes and Conway, 2008; Breazeal, 2012; Ham *et al.*, 2012; Chadwick, 2013; Fernbach *et al.*, 2013).

At the base of this structure of beliefs and practices lay the signification of immediacy as a token of qualities that made messages trustworthy. This could be used as a point of leverage to persuade message receivers to perform specific actions,

which would very according to the type of message (Hodas and Lerman, 2012; Carr *et al.*, 2016). For instance, The character sequence, “mom,” appearing on a personal smartphone may trigger the pressing of the “answer call” button; the appearance of a video with a caption reading “Live from Syria” on www.twitter.com/[profile-page] may trigger the clicking of the “Comments” button, and so on. The general and most basic rule was to believe that these messages did stand for what they meant to stand, even though relations between actors and collectivities led to the building of other, scenario-based rules (Don, 1990; Neale and Carroll, 1997). Nevertheless, just as the general rule was to accept the validity of such assumption of accuracy, truthfulness and verifiability, noncompliance came at the high price of system exclusion. In fact, doing so much as questioning the role of message construction/consumption immediacy in the individual and collective processes of knowledge construction can already cost personal and group stigmatization and partial exclusion (Martin, 2008; Helsper, 2012; Martin *et al.*, 2016). Nick Couldry and Andreas Hepp, two scholars who have developed a line of research on the concept of “mediatized reality,” succinctly explain the reason for this social expectation: “even if we do things without directly using media, the horizon of our practices is a social world for which media are fundamental reference-points and resources” (Couldry and Hepp, 2017, p. 23).

To be clear, the kind of ignorance I am referring to at this point is not based on agents’ natural inclinations, vocational and disciplinary choices or socioeconomic conditions.[13] These are also instrumentalized by the cyber-psycho-cognitive operators, yet the kind of ignorance that I am referring to is the driving factor and product of the mechanization of receiving, creating, sharing and consuming multimedia compositions.

Depending on the communicational context, people may stop thinking about language norms (Cingel and Sundar, 2012), interpersonal situational expectations constraining the relevance of message content and other details that are important indicators of agent attention (Styles, 2006; Carr *et al.*, 2016). However, even when they

[13] For a complete exploration of the notion of ignorance production, I recommend reading Robert N. Proctor’s and Londa Schiebinger’s theory of Agnotology in PROCTOR, R. N.; SCHIEBINGER, L., Eds. **Agnotology The making and unmaking of ignorance**. Stanford, California: Stanford University Pressed. 2008.

do pause to ponder about these aspects, they bypass the fundamental fact that the only “knowable” phenomena taking place at the time when the act of communication is expected to be happening are their physical interactions with an ICT device. The graphical representations of people, objects and interface elements are real in the sense that the person is witnessing them at a particular point in time and space. Yet, strictly speaking, the entities, behaviors and facts that the ICT device’s outputs are intended to represent are products of the beholder’s own interpretation; they are metaphors (Carroll *et al.*, 1988; Kuhn and Frank, 1991; Stylianidis, 2015).

Therefore, it seems to me that an instance of doubtless cognitive processing stored as “knowledge” in which the certitude of factuality is not contingent upon the direct empirical experience of the facts in question is actually an instance of ignorance production. Furthermore, when the agent expects that other agents articulate their feedback behaviors utilizing the same set of assumptions, the agent stimulates the reproduction of both a product of ignorance and the practice of ignorance production. The more compliance there is to adhere to the same logic, the more institutionalized become both the rift between “the belief of factuality” and empirical verification, and the communicational choreographies through which this rupture is performed. In turn, the system—permeated and propelled by ICT-driven practices—develops a cultural property whereby message factuality is taken for granted and, consequently, the weight of empirical verification in the processing of mediatized perceptions as “knowledge” is unconsciously lessened. Granted; not all people are careless about the fact that what they are reading, watching or listening to may not be an accurate representation of the facts, just as not all people may share inaccurate information for others to believe it is actual “knowledge.” But at a structural level, the system has developed a set of properties that not only allows for these cognitive communicational practices to turn into tendencies, but also imposes their mechanized execution for its own perpetuation.

Lowering the guard of critical thinking is not considered a defect in the mediatized world. In fact, it is part of what makes the system work at the speed at which it does. Considering digital advertising alone, how many less clicks would be generated if people were a little more prone to critical thinking? If less clicks means less money for both advertising platforms and retailers, then a market of more automatized prosumers is perhaps all-around more profitable (Google, 2019c). On the other hand, if “knowledge” standards are kept low through the maintenance of

assumptions that agents are systematically conditioned to adopt as their own, is there anything that could possibly bind media practitioners to make biased decisions in favor of accuracy, truthfulness and completeness when executing their daily job routines? Anything other than a code of ethics? These are the wrong questions. I should be asking, why were people so surprised to see “fake news” campaigns in the months preceding the American election of 2016?

The structural production of ignorance is a necessary condition to the success of cyber-psycho-cognitive campaigns because it is what ensures that “knowledge” does not need to pass through rigorous testing and verification before it can be regarded as such. Once given the status of “knowledge,” it becomes a resource for the execution of a given collective action. In the informational society, the first—and, for many, the only—type of collective action is the resharing of content with friends, acquaintances or the public at large using digital communication channels such as email and social media platforms. From this point onwards, all the people with access to the shared constructions become “knowledgeable” of whatever object-attribute relationships were represented through them. Interpersonal trust and source familiarity prepare the individual’s psychological state to settle for these definitions, even if in some cases this acceptance is preceded by a prior comparing-and-contrasting exercise involving constructs from alternative sources (Giffin, 1967; Holton, 1994; Jones, 1996; Keren, 2014). Hence, the messages reach a status in which they are treated as if they were “knowledge.” After they get reshared a few hundred thousand times through chains of people who trust one another, the entire network of networks—society—becomes readily mediatized with “knowledge”—ignorance!—of whatever was represented through the constructs.

3.2.2. Production of ignorance induced by machine recommendations and machine exclusions

Mediatized reality’s structuration has other rules and mechanisms for the articulation of “knowledge” besides the ones analyzed in point 3.2.1. Instead of concerning itself with people’s cognitive-behavioral approaches to the construction/consumption of online multimedia messages, the set of rules discussed in this section addresses the conditioning of the content resources’ probabilities of reaching the point where they can enter the mechanized, multi-party, communicational

choreography. They regulate the chances of content items emerging from the vast seas of "information" up to users' field of view.

"Regulated views" entail regulators, exclusions and subordinated viewers, for inclusion and exclusion occur concomitantly and automatically in every eye-screen interaction. Exercising the hegemonic leverage of its search algorithm (Brin and Page, 1998), Google molded the web's inclusion/exclusion logic based on the notion of personalized relevance and "knowledge" authority.[14] Recalling from earlier in this dissertation, this means that results are ranked in descending order according to two topic-related variables: contextual relevance and authority ranking. Currently, contextual relevance is a measure that compares the search engine's "understanding" of the user's underlying intent at the time of executing the query and Google's index of the "knowledge" available in the Internet. Google's "understanding" of the user's intent is only partially based on the user as an individual. It is to the extent that it takes into account signals that describe the context in which the query is performed (e.g., location, operating system, type of device, hour of the day, etc.), data points gathered from the user's profile (gender, age, places visited, etc.) as well as historic search and web navigation data (past Google and YouTube searches, web pages visited in the last X days, etc.). But it goes beyond the individual when it uses the above to construct a transitory user profile that allows it to relate the user's query to cohorts of similar users who have made similar queries in order to observe the segments behavioral tendencies when faced with specific search results assortments (Simmons and Catanzaro, 2012; Cheyer *et al.*, 2015; Yan *et al.*, 2015). Google monitors what happens after users click on one of its search results and "land on" the corresponding page. It observes users' consumption of the website content, reading multiple signals to evaluate whether the user is having "a good experience." If so, then Google predicts the website's entry page should be listed as a relevant source every time a user from the segment in question executes a similar query.

Although the listings' appearance at the top of the search results page is intended to convey Google's "understanding" of the user's intent at the time of executing the query, Google's calculation of the degree of relevance that web pages

[14] If Google was a purely-scientific index comprised of peer-reviewed publications, then I would choose to write the term, "knowledge," without quotation marks or change it altogether to refer to "scientific authority." The idea is somewhat similar to the basic bibliometric principle that the more times a work is cited by other works, the more relevant it is. If the works citing it are themselves highly cited works, then their inbound links indicate even greater scientific value.

have vis-à-vis specific search terms takes into account more than “similar” users’ “landing page experience.” Just as users are contextualized within cohorts of “similar” users based on permanent and dynamic variables that define them as individuals, Google also evaluates specific structural and transitional web page elements to evaluate both their semantic value and their “knowledge” authority positions within a network of pages about the same topics. Structural page elements are common to all but differ in their semantic value; they include URLs, titles, headers, meta descriptions. Transitional page elements vary from one page to another; they include alternative text descriptions designed to increase the accessibility of images for visually impaired users, as well as links pointing to both the page itself (i.e., “inbound”) and other pages (i.e., “outbound”). As highlighted earlier in this dissertation, inbound and outbound linking is one of the mechanisms with the greatest impact towards the reinforcement of both the positioning of certain entities as topic-based network “authorities” and, by the same token, the institutionalization of specific definitions as “knowledge” about their topics of “expertise” (Kleinberg, 1999; Zhu *et al.*, 2011; Traphagen, 2018) It works in a similar fashion to how it works in academia.

The citation of an expert’s work in a publication of another expert in the field may indicate relevance in the field. More citations from experts would probably indicate an even greater degree of importance to the field. The “scientific legitimacy value” conferred by these citations is bound to increase even more if the works citing this work earn citations from other known scholars as well. A steady number of citations for the years to come may signal the timelessness of the work’s relevance to the field. However, perhaps way before this, as the scholar has gained substantial credibility as a scientific authority, his other works would reap some of the benefits that come with it: scholars and students alike starting their reading under the mindset of someone who believes that whatever is printed in those pages can be called “knowledge,” people asking about future titles, perhaps even a fanbase. But who knows if this renown scholar would have ever come to be recognized had his work never been cited by anyone other than his unpublished undergraduate students? After all, their works may have never been read by anyone other than their scholar professor, thus, the chances of their research papers increasing the visibility of the scholar’s own work before an audience of other renown scholars are rather low.

As the Internet’s search hegemon, Google defined the rules such that, in “the academic field of the Internet,” web pages—represented by the scholarly publications

in the allegory—are assigned topic-based “knowledge” authority scores based on the number of inbound links, the topics of the web pages corresponding to these links, and their own “knowledge” authority scores (Brin and Page, 1998; Page *et al.*, 1998). The greater the number of high-score-page inbound links, the greater the receiving page’s “knowledge” authority score. If this page links to another page about the same topic, it confers credibility value to the receiving page. If, on the other hand, it links to a page with a low relevance score, the linking page and its website—the allegory’s scholar—could be penalized. This leads to a form of authority-based stratification in which content creators may link to pages in domains of equal or higher authority levels but restrict their links to websites at lower levels of authority. As Google set the rules so that top-of-page ranking probability increases with higher “knowledge” authority scores, then the semantic value of any given query—the end result of a cognitive process involving questioning, query wording, results recognition, click selection, page landing and content discovery—is defined among the same set of domains. Moreover, since websites tend to link to other websites in equal or higher “knowledge” authority categories and these are directly linked to topic relevance, their definitions of the same topic cannot be very different from one another; they tend towards topic uniformity. Taken together, these rules structurate search results pages whose top is composed by semantically homogeneous, “knowledge” resources, provided by a handful of mutually referenced content creators.

Furthermore, as for any given query the search results with the most clicks will stand a higher chance of accruing sessions indicating “good quality user experiences,” the websites with higher “knowledge” authority rankings also have more opportunities to deliver such type of session. The more they do it, the wider the range of possible “similar” users grows. This has the effect of multiplying the size of the audience through sheer “similarity.” As for their semantic intent, it may not necessarily be as “similar,” but it is conditioned into uniformity by the options shown to them in their field of vision (Kahneman, 1973; Eysenck, 1982; Styles, 2005; Hodas and Lerman, 2012). All of these “alternatives” may seem different but when it comes to defining their topic, they are essentially the same. Thus, ignorance is structurally produced: users have placed requests for knowledge with nuanced intents and in return they have got uniformed definitions, pushed to them as the most relevant matches possible. The hegemonic, scientific-authority-like figure attesting to the reliability of the “knowledge” served makes them believe the results are truly what they stand for given their position on the

page. Yet, in fact, what they really are is the most “normalized” results possible given both the topic of users’ queries and the cohorts that Google has placed them in to establish the probability of relevance as a function of landing page user experience. But users do not know this, much less do they wonder if the results match their intent or if it is their intent that is being shaped to fit the results that the search algorithm surfaced to their field of view. While not all data-driven recommendation contexts are structured as lists of search results, their logic is based on the relevance and authority principles utilized by Lawrence Page and Sergey Brin to devise Google’s PageRank algorithm.

Machines’ act of recommendation is one of fulfilling a specific agenda by narrowing down a set of possible courses of action while conveying a rationale for the decision-maker to choose one of the alternatives. And the metaphor that mechanizes this process at the most fundamental level—the gateway to the web; the hub of definitions—and in the most subtle way—a higher or lower placement on a ranking—is Google’s search results page. Retrieving third-party content to configure the user’s onscreen field of view according to points of convergence between calculated assumptions about his or her interests and possibly relevant alternatives to move the interaction process forward is Google’s core design logic. Furthermore, it was Google that conditioned the reproduction of such logic as the foundation for the Internet’s information architecture standards and as the driving force behind the dynamic generation of personalized user experiences. This hegemonic power stemmed from its monopoly of the online information search market, which acquired thanks to the unparalleled robustness, efficiency and effectiveness of its search algorithm—facts from the late 1990s that still hold true today, more than twenty years later.

3.2.3. Construction of a searchable data realm of syntactic and semantic relationships

As stated earlier in this dissertation, cyber-psycho-cognitive operations emerge from latent environmental conditions. One such type of condition is the ongoing construction of a searchable data realm of syntactic and semantic relationships. You and I take part of this process every time we search for—what we expect to be—knowledge about concepts, objects, events, people or anything else that can be referred to using search terms. “Search terms” are nothing more than specific character

sequences—chains of zeros and ones, if you will—that we submit for search engine analysis with the expectation that the machine will respond by providing a list of results sorted in descending order of relevance, following the logic explained in point 3.2.2. The clicking choices we make next add up to the statistical probabilities that the search engine will consider when calculating the intent of the next batch of users making queries using similar search terms. However, as was discussed, there are structural factors that make the definitions articulated by certain "knowledge providers" appear much more frequently in the screen regions where the statistical probability of user clicks is the highest (Caphyon, 2019). This graphical prevalence results in the programmatic generation of bias in favor of their "knowledge" contributions towards the semantic value of users' search terms, granting them either perpetual predominance or absolute monopoly.

Nevertheless, the above just summarizes the first stages of the construction of the searchable data realm of syntactic and semantic relationships. As ICTs became capable of serving increasingly personalized roles in both collective and individual activities and environments, they were put to the test as facilitating tools in a myriad of intersubjective scenarios for communicative action.

Machines did not disappoint. They developed protocols to share user-generated, semantic data across the blogosphere, web portals, online search and socialization platforms (Mayer and Mitchell, 2012; Gomer *et al.*, 2013; Manolarakis *et al.*, 2014; Mai, 2016). This datafication process permitted the construction of semantic-based narrative conduits across entire user sessions and beyond (e.g., searching for a word on Google would trigger relevant email ads, Facebook sponsored content, similar ads on the right margins when buying movie tickets, etc.). Machines also increased the robustness of their neural networks to accommodate the interpretation of emerging syntactical structures such as tweets, hashtags and emoticons, while also learning to distinguish the sentimental nuances behind them (Liu, 2012; Rosenthal *et al.*, 2014; Tang *et al.*, 2014; Zhao *et al.*, 2014; Liu, 2015; Guha *et al.*, 2016; Healey, 2017). As stated in previous sections, this seemingly-simple enhancement added psychological depth to user profiling in machine-readable formats that were perfectly adequate for audience segmentation and microtargeting (Murray and Scime, 2010; Barbu, 2014; Yan *et al.*, 2015; Schipper and Woo, 2017; Borgesius *et al.*, 2018). Adding to the semantic enrichment of machine data, neural networks' advancements in semantic-recognition capabilities in non-text media have also allow them to derive

datafiable meaning from image, audio and video files posted by users (Cambria *et al.*, 2013; Gajarla and Gupta, 2015). And even when it is not posted by them, machines have been equipped with image, audio and location sensors that automate the transmission of context-related information (Ritzer, 2015). These data signals complement the meaning of the syntactical constructs that users consciously provide to the online systems their logged on. Even user states, which are not supposed to be communicative actions in and of themselves, have become communicative.

Whether it be through properly constructed sentences on search boxes, 280-character sequences on tweeting fields, emoticon-packed WhatsApp messages, hashtags, or unbeknown, background reporting of "frequently-visited places;" machines love to hear from us. This is how they began to learn what specific character sequences were used for from a grammatical standpoint. Now they know the usual meaning of words, their possible alternative meanings, when people convey the same meanings without using proper grammar and the sentimental tendencies associated with specific character sequences (Barbosa and Feng, 2010). They also know how the words are pronounced, how to understand audio and type the words they hear, and they are also getting better at deriving sentiment semantic value from image, video and audio content (Kaushik *et al.*, 2013; Wang *et al.*, 2015; Poria *et al.*, 2017). As machines can integrate all dimensions of the user's contextual data—from the last few hundred searches, to current sentimental state—fulfilling the promise of building consistent experiences of "relevant knowledge" should be attainable.

But there is a missing piece in the puzzle: what is the incentive behind putting together, maintaining and enhancing these expensive ensembles of neural networks serving what appears to be for the most part "free" content? After all, most services just ask for basic personal information. Apple Inc's CEO, Tim Cook, summarized it well at a keynote address at the EU Parliament in Brussels on October 24, 2018:

> Our own information, from the everyday, to the deeply personal, is being weaponized against us with military efficiency (…) These scraps of data (...) each one harmless enough on its own (...) are carefully assembled, synthesized, traded, and sold (…) We shouldn't sugarcoat the consequences. This is surveillance. And these stockpiles of personal data serve only to enrich the companies that collect them (Cook, 2018).

Cook points out the missing piece in the puzzle, which is the value of the data being collected, extracted and derived by the machines; its function. It can be incrementally enhanced through semantic enrichment and become more expensive, but this does

not change the source of its value; it always comes back to how it is utilized. Cook delivered his speech in the context of a wave of public debates about data privacy policy sparked by the Facebook-Cambridge Analytica scandal (Kang and Frenkel, 2018), which uncovered one of the socially-engineered data sources of the Trump campaign. Therefore, the "weaponization" and "military efficiency" he describes is no other than that of the messages employed in a cyber-psycho-cognitive operation.

> We see vividly, painfully how technology can harm, rather than help. Platforms and algorithms that promised to improve our lives can actually magnify our worse human tendencies. Rogue actors and even governments have taken advantage of user trust to deepen divisions incite violence and even undermine our shared sense of what is true and what is false. This crisis is real. It is not imagined, or exaggerated, or crazy (Cook, 2018).

This data realm is "searchable" for all, but not in an equal capacity. As the owners of the "platforms and algorithm that promised to improve our lives," the data acquirers and generators have first-hand access to it. Mainstream media can buy "stockpiles of personal data," or simply rent the artificial intelligence marketing platforms with the capability of getting the message in front of the right audience "with military efficiency." Political parties become clients of both platform owners and mainstream media to pursue the preemptive erosion of their adversary's legitimacy and secure the legitimation of their own authority, even it means precipitating a socio-systemic crisis through social polarization. In the meantime, Section 702 of the U.S. Foreign Intelligence Surveillance Act allows the State to search and watch how it all unfolds (United States, 2008). It captures user communication data from both U.S. Internet and telecommunications infrastructure (i.e., "upstream collection") and U.S.-based service providers such as Google, Microsoft, and Apple (i.e., "downstream collection"), thereby exerting hegemony over the data acquirers' and generators' own AI-powered machinery. The picture I see is one where there is a super surveillance system overseeing and feeding on the output of the technological capabilities of another. If so, the super surveillance system would be in the position to make "an orderly sense" of society, while influencing the behavior of social segments through the conditioning of the messages they are bombarded with. Quite an Orwellian picture, I am afraid.

3.2.4. User journey machine-learning

The machine-assisted process of weaving a realm of syntactic and semantic relationships was propelled by the interplay among the main power agendas regarding the utilization of its constituent data. At the most basic level, all agendas share a data-driven surveillance function,[15] but not all of them have the submission of an audience to a programmatic transformational experience—a "user journey"—as one of its main objectives; this is a key characteristic of cyber-psycho-cognitive operations. As stated earlier, the State is the opaquest of all actors involved. Due to this, there is not enough information to learn the communicational strategies implemented by intelligence agencies in order to have individuals develop specific behaviors of strategic interest.[16] Hence, while I can acknowledge the scientific potential of studying the construction of, for instance, self-censorship-oriented, cyber-psycho-cognitive operations, this undertaking seems infeasible for the time being. The world of digital marketing, however, is very open about the types of strategies and tactics it employs to turn users into a brand's "evangelists" after performing a series of actions on its digital channels.

During the past twelve years, one of the industry's top contributors to the perfecting of these user-experience-based, psycho-transformative mechanisms has been web analytics expert—and Google's official evangelist—Avinash Kaushik. With Google's endorsement, his "See-Think-Do-Care" (STDC) framework for "customer-journey" management has become the leading standard for the mapping of intent-based audience clusters and the configuration of matching programmatic, business-oriented, communicative actions (Kaushik, 2015). Each of these communicative actions is designed to make the cluster members from one stage to the next. "See" the brand if they have not. "Think" about consuming what the brand sells, if they have only "seen" the brand. "Do" what the brand asks them to do if they have only "thought" of doing it. Once they are "done" with all of this and have completed two or more

---

[15] Even prosumers use of social media platforms and search engines bears similarities with certain types of surveillance. For instance, people can spend countless hours looking up references to other people, events, videos, images and other content sources that awaken their curiosity, linking from one reference to the next, following a chain pattern. Although this is not the same as real-time activity monitoring, it is similar to spying.

[16] This is by no means to be interpreted as the implausibility of such program's existence. In fact, it would not be the first time that the U.S. sponsors a program to develop "mind-controlling" capabilities to effect behavioral changes in people considered threats to State interests. For instance, from the mid-50s to the late 70s, Project MKUltra worked in developing and testing methods to accomplish this.

transactions, then they should “care” about the brand. The brand “evangelist” is the one “caring” individual who is fervent and loyal to the brand; a magnet for “seers,” “doers,” “thinkers,” and a source of inspiration for fellow “care givers.” Of course, the gospel is spread through Facebook and Instagram posts, WhatsApp groups, tweets, YouTube videos, forums, niche blogs, LinkedIn articles; every single space that allows for a few compelling words raving about the brand and an outbound link to one of its digital properties. Audiences click on these links, the land on the digital properties’ pages and they become automatically “registered” in a “remarketing list”—a type of audience including users to be periodically targeted with a distinct set of messages, crafted according to the stage that the system has identified they are in based on the rules that marketers have configured in advance. You are probably thinking, “This has happened to me, but how is this even possible?”

As it has been suggested in previous sections, websites of all kinds—from services with native AI capabilities, to simple newspapers or blogs—use mechanisms to record the data points that characterize users as unique online agents. These mechanisms are commonly known as “persistent cookies” (Acar *et al.*, 2014). They are unique-ID, expiration-based, data files that websites use to provide experiential continuity in one-to-one user relationships that may evolve through intermittent interactions along an extended period. Websites’ servers produce these files and send them to users’ browsers for local storage. Although the files themselves do not contain much information, website servers use their unique IDs as keys to associated server-side files in which they record the values for the variables describing the state of the user experience at the time the user ended the last session. The next time the user visits the website, the server requests the cookie file from the user’s browser and hence fetches the user’s data using its unique ID. Once it accesses the data and identifies the values that were recorded at the end of the last session, the server can recreate the last relevant state, thus moving the website-user interaction process forward. Some websites

This is how the general mechanism for the recording of user journey events works. It is instrumental to those who can search the data realm of syntactic and semantic relationships not only because of the types of user dimensions it facilitates the datafication, integration and quantification of, but also because it allows them and other third parties to partner up with websites all over the Internet in the collection of user data for sale to advertising services (Vázquez *et al.*, 2014; Chang and Kannan,

2015). The list of collectible data points is too long to cite them all in here[17] but, for the purposes of the current discussion, suffice to say that they can track and combine all variables pertaining to time, space, device, medium, channel, campaign, ad content, referrals, entry and exit points and, of course, the keywords used to both reach and search inside a website. It would be cause for alarm if "information, from the everyday, to the deeply personal, [was] being weaponized against us with military efficiency" (Cook, 2018) to pay higher health insurance premiums or mortgage rates (Chen, 2019; Wheeler, 2019). Sadly, it does not end there. If health maintenance organizations (HMOs) and banks can become data acquirers' and generators' clients, so can political parties. The difference in the clientele lies neither in the systems they use, nor in the "user journey" frameworks that their marketers utilize while managing their advertising campaigns—they all have users walk down "See-Think-Do-Care" road with the help of digital marketing platforms. Rather, it lies in the nature and intensity of the communicative rationalities that would typify "seeing," "thinking," "doing" and "caring" in the context of a cyber-psycho-cognitive operation.

As the American presidential campaign of 2016 showed, the communicative rationalities of cyber-psycho-cognitive operations are characterized by centripetal forces that quickly incorporate individuals into daily cycles of collective actions, fluctuating from the virtual to the physical realms of experience through the versatility afforded by mobile technologies (Borge-Holthoefer *et al.*, 2016; Matsa and Lu, 2016; Granberg-Rademacker and Parsneau, 2018). These virtual and physical socialization practices would alternate in micro and nano cycles, evidencing groups' concomitant online and physical community building through the construction and instant mediatization of collective content (Alashri *et al.*, 2016). A family of campaign-selected hashtags based on "linguistic bait" played the role of the "discursive center" of the centripetal force, providing the "semantic magnets" for both "discursively-aligned" movement growth and data-driven audience segmentation and microtargeting discursive construction participants (Vosoughi, Vijayaraghavan and Roy, 2016; Groshek and Koc-Michalska, 2017; Hendricks and Schill, 2017). Thus, community-

[17] See Google Analytics' list of dimensions and metrics to get an idea:
Google. **Dimensions & Metrics Explorer**. Mountain View, California. Available at: https://developers.google.com/analytics/devguides/reporting/core/dimsmets. Accessed on: May 22, 2019.

building in the physical public sphere became an organic online recruitment activity in and of itself, being carried out through platforms that were either born or had evolved into predominantly mobile channels such as Twitter, WhatsApp, Snapchat, Instagram and Facebook.

In this sense, the challenge that cyber-psycho-cognitive operation strategists face is twofold. On the one hand, they are confronted with a challenge that is not all that different from the one that political campaigners used to tackle prior to the rise of deep learning ICTs: gaining and maintaining the orchestration capacity of the campaign's fluid communicational environment, even when it is not fully controllable. On the other hand, they also face a challenge that is unique to their age: making sense of the obfuscating amount of data and information that characterize the fluidity of their communicational environment However, I would argue that the information systems that help user journeys emerge out of the depths of the data lakes—the managerial side of the "system of permanent registration" (Foucault, 1995, p. 196)—allow strategists to overcome both. As third-party cookies collect and compile the key bits of people's online discursive activities, strategists can now "outsource" the gathering of audience feedback to deep learning machines capable of understanding the sentiment semantics encoded in natural language expressions spread throughout the web. Web analytics platforms can integrate these data and output views where the dimensions collected through third-party cookies are quantified in a variety of metrics. Once there, strategists can observe the users' journeys and understand what their communication efforts in all channels are accomplishing on the ground. The possibilities of what they can do from there are endless.

For example, studies indicate that during the American presidential campaign of 2016 it was perfectly possible to pinpoint the association between and among keywords, topics and sentiments using natural language processing technologies and Twitter data (Vosoughi, Vijayaraghavan and Roy, 2016; Vosoughi, Vijayaraghavan, Yuan*, et al.*, 2016). This means that sentiment trends could be analyzed in the context of trends whose linkages to discursive construction events can be directly established; time, location, device, ad content, marketing campaign, segment, to cite a few. The challenge for political party marketers then becomes defining data-verifiable, communicative action measures of "successful journey-phase completion" and continuously monitoring how the feeding of "objective knowledge" stimulates the

communicative rationality outcomes that tend to conduct people towards the next stage in their journey.

To continue with the Twitter example, analysts identified that most of the people whose tweets reflected emotions of fear and anger tended to use keywords related to topics such as “immigration,” “job security” and “national security policy” (Liberty, 2017). A cyber-psycho-cognitive operation strategists could have taken this information, and both reconstruct the “discursive origins” of this segment and observe the activities that its members did after posting the tweets under analysis. For example, they could have queried data from all of their digital properties to try to pinpoint users whose journeys included twitter.com as last or second to last step before landing, and who used the keywords under discussion on the dates, times and places matching the sentiment-oriented analysis. Then, they could have configured a custom segment in their web analytics system. Once this “entity” exists, they can track its journey the way they would a single user’s, except of course it will not have absolute events (e.g., “user X went from A to B then to C”) it would have trends instead (e.g., “75% of users in this segment went from B to A; 10% went from A to B; 5% went from B to C and 10% went from A to D). Furthermore, they can also have the web analytics system create an “audience entity” out of the custom segment and feed it to the digital advertising system and let it grow according to the number of new cookies that fit the same pattern. Once the audience grows to a certain size, the digital advertising system will automatically create an additional audience containing “similar” users (Google, 2019a; b). These audiences can be used as ad targeting mechanisms, which means that, provided that the ads’ messages are effective at leading audience members to carry out the communicative actions that will bring them to the next stage in their journey, the system will likely succeed at one point or another. In the end, the challenge lies in defining the expected behavioral outcomes for each stage. Since all of these are in fact sub-goals in an overarching strategy, it seems to me that marketers should probably approach this as a reverse-engineering task: learn the cyber-psycho-cognitive operation’s end goal and work their way back.

4. HIERARCHICAL CONSTRUCTION OF CYBER-SPATIAL POLITICAL NARRATIVES: BUILDERS AND DESTROYERS OF LEGITIMACY

The incorporation of virtual robots empowered with artificial intelligence (AI) as additional agents in the structuration of social and cognitive experiences on cyberspace has introduced both complexity and risk to one of the most fundamental processes required for the effective exercise of power: the intersubjective construction of legitimacy. The connection between virtual robots with artificial intelligence and political legitimacy begins with the way in which the public knowledge on which legitimacy is built is produced on cyberspace. Clearly, knowledge is not generated in a vacuum, it is articulated and validated through socialization (Berger and Luckmann, 1966), and cyberspace is the most pervasive realm of socialization of our time (Castells, 2010b).

Socialization on cyberspace happens through narratives. I synthesized a taxonomy of narratives based on my personal observations and practical experience.[18] First, there is "the object narrative." Object narratives refer to virtual objects with archetypical graphical attributes that are fundamentally persistent, yet customizable (e.g., a box-like object with the words "log in" typed in it is a button that triggers the submission of credentials for system verification. The button can be in any color, appear in thousands of websites, on different screen regions; its functionality does not change, our beliefs regarding what it does remain the same and so does its narrative). Built on top of this family of functional narratives there is a second kind; "the object-user narrative." Object-user narratives are choreographed human-computer behavioral exchanges and they manifest as reaction sequences between system and user (e.g., the narrative of how hitting the "enter" key after typing a sequence of characters beginning with "www." and ending with ".com" in the long white box that appears near the top of the web browser window could lead to a reconfiguration of the

[18] During the past fourteen years, I have exercised several professional roles in the web marketing industry. This experience has helped me develop considerable knowledge on the theory and practice of software design and development, business analysis, digital marketing strategy and campaigning, web analytics, search-engine optimization (SEO) and user experience design. Hence, I am fully confident that I can make a well-informed synthesis of the main types of narratives that condition everyday cyberspace interactions. There is no doubt that it can always be improved. However, this condition does not necessarily invalidate the synthesis I put forward, for improvement is in science's nature.

visual elements on the screen such that it would appear as though there was a displacement from one *place* on the web to another). Object and object-user narratives enabled provide the building blocks for a third type of narrative; “the user-system-user collaborative narrative.” They occur when two or more users converge on a communicational context that is designed for them to participate in collective content creation processes. This takes place within a framework of information architectures, tools and mechanisms conditioning both the inputs and outputs of the process, as well as the users’ performative tasks options. Although at the abstract level these frameworks utilize architypes that are mimicked and recreated beyond the confines of any one proprietary interaction context, each instance tends to be owned by the platform that hosts it (e.g., Facebook’s *news feed* is Facebook, Inc.’s; from an abstract point of view, Twitter’s “timeline” shares some of the functional features of Facebook’s *news feed*, yet it is Twitter, Inc.’s). However, two aspects that are common to all is the stimulation of socialization and the platforms’ participation in the overarching structure defined by the logic of “relevance” and “authority,” both of which are manifestations of solicited and unsolicited system outputs to mechanical interpretations of users’ contextual interests.

Thus, the three basic functional narrative scenarios described above are embedded in discursive environments that promote the satisfaction of private interests through the creation and consumption of knowledge. Whether individually or collectively, this search for satisfaction through knowledge-oriented activities rarely happens anonymously. Just as in most physical settings, people socialize using avatars conditioned by a combination of factors including their end goals, others’ expectations, places’ explicit and implicit codes and the available resources. This is the fourth type of narrative, the online avatar, configured according to a somewhat similar logic. People become a social platform’s users if they so wish—albeit these days not being a user in any capacity is nearly synonymous with socioeconomic exclusion—and, as users, they create profiles. These profiles are composed of system-defined variable ensembles configurable from a mixture of machine- and user-defined values. Although the system requires the user to provide values for most variables, there are usually some that are completely or partially optional. Furthermore, as platforms, profiles and functionality usages have gradually become more sophisticated, profiles have tended to add more layers of information for users to enrich

their personalization. The avatar is in and of itself a narrative; a metaphor of a person. But other narratives emerge from the power of this metaphor.

One of them encompasses users' beliefs and expectations regarding the extend and reach of the avatar's capabilities as a virtual object and how these translate to magnifications of their own communicational capacities; the narrative of "the avatar's capacities." It is founded on and confirmed through the user's experience of the avatar's communicational functionalities, which tend to vary from on web service platform to another (e.g., users can post messages longer than 280 characters on Facebook, but not on Twitter; users can stream live video on YouTube, Facebook and Twitter, but not on Pinterest, etc.). However, one of their common properties is to leverage web-service-platform cookies to extend their functionalities beyond their original domain, for instance, every time an outside website allows the user to use a specific platform's avatar to interact with its functionalities (e.g., form completion, commenting, new profile creation, etc.).

Functionalities lead to expectations on the part of any user involved in a given dialogue, both from the meddling system and the other user participants. People expect that others can have their avatars perform the same functions as their avatars perform. Catering to this expectation entails accepting all the assumptions underlying the workflows necessary to make avatars produce the same behaviors (i.e., the assumptions implicit in the previous narratives). Acceptance is a critical point in the process of generating information trust from user interaction. It is by accepting all previous functional assumptions that users can turn the information interaction process into an automatized experience, wherein obtaining the "expected" results depends on the repetitive execution of unequivocal methods. Since failure to do so results in the breakdown of the communication flow, and acceptance and repetition produce the "expected" results from both system and users—who have agreed to the same terms—people opt for the latter. This generates user trust in system-mediated communication and in the information it outputs. Trust, too, eventually becomes automatized.

Moreover, as a person's digital representation, an avatar's discursive characteristics creates a narrative that I call "the narrative of avatar individuation," which in fact operates as a sociopolitical discursive transfer channel of two directions between the individual and the avatar. The person projects on to the avatar his or her socially-known individuating characteristics and these condition all aspects of his or her social network, both as a matter of personal choice and as a result of the

application of machine recommendations. Furthermore, the avatars in the avatar's audience treat it the way they would treat the person in the physical world, just as they expect that the avatar's behavior performs according to their memory of the person's behavior. On the other hand, what the avatar does online has an effect in the life of its administrator, for people understand its existence as an extension of the person in the physical world. Comments made, links shared, friends made, friendships broken; it all reflects back to the person's life for better or for worse.

Following a similar logic, there is a type of narrative that is specific to political authorities' avatars, I call it "the narrative of political personification." Beyond the right to the legitimate use of force, political authorities' legitimacy grants them discursive power privileges that no other type of social figure has. These privileges range from access to audiences with decision-making power to enact laws and execute public and foreign policy decisions, to the use of the symbolic power of the authority figure to communicate tacit approvals for social behaviors that would otherwise be unacceptable or even illegal. One of the common denominators underlying these explicit and implicit prerogatives is public trust; as long as they are "perceived" as "legitimate" authorities, they will continue to have access to these privileges. Avatars inherit these perceptions of "legitimacy" as if absorbing its properties through discursive means. Thus, the discursive powers that do not require the involvement of legal procedures to be manifested can be projected through the digital avatars. For example, a president may announce policy decisions made regarding the future, instantly reaching millions of people around the world and possibly accelerating their impact in other countries' policy-making decisions as well. However, he cannot turn words into law by simply posting a tweet—at least not as of today.

Much like political authorities, knowledge authorities' avatars carry the weight of the knowledge power and reputation of the person or institution they represent. Their avatars would exemplify "the narrative of knowledge authority." Although scientists' avatars would fall in this category, the type of institution that has the greatest outreach and attributes to itself the fulfilled duty of providing information and facilitating the articulation of knowledge is the news media outlet. Their legitimacy does not emanate from a public decision, but rather, from the continuous feeding of content on topics of "current relevance" which gains credibility and public trust when synchronous with what other news media outlets are feeding. In the age of search algorithms, this agenda-setting dynamic is recreated through topic- or issue-based, cross-domain URL sharing.

This increases their authority ranking scores for specific trending searches as well as their chances of appearing in the top positions of the list of search results in Google and Bing. Once at the top, the probability of users clicking on their URLs is much higher than that of any competitor's ranking below the second or third positions. The more the pattern repeats itself, the stronger becomes the belief that what these outlets publish is indeed "the facts," "the truth," and "what is relevant at the moment."

Both the discursive legitimacy emanating from politicians' avatars and their frequent expressions of political discourse, as well as the trust and reputation carried over by mainstream news media outlets perceived as the holders of access to trustworthy information and knowledge had a compounding effect on the perceived nature of social media. This was parallel to the effective transformation of the Internet into a worldwide ecommerce realm, which demanded heavy investments on the construction of not only ecommerce-oriented, cybersecurity infrastructure, but also the discourse necessary to elicit trust from the public. And the marketing efforts paid off; public trust in the security of the Internet grew as a whole as more people began to get the products they ordered online, and less people complained about getting their IDs and credit card numbers stolen. This discursive environment gave rise to what I call, "the narrative of online information trustworthiness."

As information constructs, this narrative incentivized the institutionalization of avatars as valid, literal, socially-accepted representations of people. For the same reasons, social media had ceased to be a mere "playground" for nonchalance and informality and had become a reflection of the public sphere. As such, it also reflected people's trust in the people, entities, processes, structures and systems they trusted in the physical public sphere. Thus, "the narrative of online information trustworthiness" also disseminated a construct about social networks themselves; they became spaces where avatars could have access to trustworthy advertisements, trustworthy information from genuine representations of reputable knowledge sources, and expressions of political discourse that came from the authorities themselves. This is the atmosphere of trust in which, thanks to the power of spacetime compression, avatars invested in public and/or personal trust share "live news." They may not be more than a line of text, they may embed images, "live video" streaming frames; social media posts are at least representations of the content sharer's own epistemic phenomena at the time of publication. The content sharer's audience trusts in this immediacy and, when the content expresses messages referring to a context, they

also tend to associate his or her opinions with facts about the context—because they trust the content sharer's judgment. Essentially, this is how "reality" becomes represented, mediatized, framed as facts and believed as such; all in real-time. The underlying mechanism is the mediatization of reality; I call the narrative that makes people prone to granting "knowledge status" to the representations of reality, "the narrative of instantly mediatized facts."

People's acceptance of this narrative is of outmost importance for both news media outlets and political entities (i.e., State agencies, parties, politicians). It is based on two concomitant phenomena. On the one hand, there is the narrative of online information trustworthiness, which provides a composition of "trustworthy" avatars and contextual elements to choreograph a digital *mise-en-scène*, a trusted channel, a trusted anchor, trusted State officials, analysts, politicians, places that appear to be the places being described or referred to, etc. On the other hand, there is the mirage of immediacy, which has all these "trustworthy" *mise-en-scène* elements perform their roles and have their dramatizations be instantaneously datafied and transferred in real-time through the network infrastructure on which the informational society is based. The message receiver has no first-hand, empirical proof that the digital avatars in the consumed scenes are in fact the people they purport to be, but the people that they represent, the channel bringing the news and the medium on which the experience is being lived are all "trustworthy," "therefore, it must all be real and true." This compounding of narratives, expectations, beliefs and chains of trust make for fabulous quid pro quo opportunities between mainstream media and political figures.

One of them is the instantaneous mediatization of a façade of institutional transparency through the insertion of expressions from "trustworthy" "insider experts" as sources that "can attest the veracity" of "X" o "Y" on behalf of the person they represent, who is himself/herself a representative of some agency, institution, company or news outlet. These are the modern-day "knowledge experts" that Max Weber spoke of in his theory of administrative secrecy. They are avatars of people positioned "closest to the source of truth," "closer" to the reporter or journalist on site, somewhat distant from the newsroom, and "furthest" from the audience. "Luckily," the audience has the news outlet to bring "the facts and the truth from so far away." Unfortunately, if knowledge and certainty of fact were the measures of distance, perhaps the actors sharing "information" with the public would end up being much closer to the public than they seem to be, especially if the chain of "knowledge sharing"

ends and begins with declarations of the type, “sources say” and “experts think.” For claims such as, “the Russians are helping Donald Trump,” these types of statements do seem rather shallow in terms of “epistemic depth.” But in the end, it all works out for the talent running the show. Political avatars maintain the public thinking that “they disclose” factual information. This public belief in transparency, reinforces its belief in the veracity of the “information” it is fed; the seeds of the myth of political accountability are sown. Furthermore, as this spectacle of transparency is not optional in modern democracies—accountability is supposed to be one of their key properties, therefore, it must exist, even if just as a mirage—delivering it to the devices of every citizen is an all-around profitable business. First, constructing political “transparency” before the audience generates trust and credibility capital for “bringing the truth from the trenches”—which gets “reinvested” one news cycle after another. Moreover, as news media outlets perform the role of “the middlemen” in the information-supply chain, audiences have no choice but to “buy their product”—and they pay for it by viewing and clicking on ads. Furthermore, there are no alternatives to this mediatized experience of political life (Lippmann, 1997), for even when “disconnected,” offline political discourse revolves around references that exist in mediatized reality (Couldry and Hepp, 2018). In fact, it is no exaggeration to say that even beyond politics, this has become the way to experience the world, “(…) life is presented as an immense accumulation of spectacles. Everything that was directly lived has receded into a representation” (Debord, 1992, p. 7).

This has given news media outlets the capacity to define “the key issues and topics of the day and (…) to influence the salience of these issues and topics on the public agenda;” a mediatic function which has come to be known as “agenda-setting” (McCombs, 2014, p. 1). This role is anything but new. The issue of the industrywide homogenization of the news into a predefined set of salient topics was addressed as early as 1947 by the U.S. Commission on Freedom of the Press (Rogers and Dearing, 1988, p. 557). In practice, it operates as a metanarrative about the news narratives’ degrees of importance vis-à-vis the public. It is tacitly introduced through cues that indicate relativity of topic salience. In newspapers, they include headlines, colors, font sizes, page-space allocation and story placement within the day’s paper. In TV newscasts the frame composition logic inherits some of these basic principles, but it is by and large different because they are based on a moving-image medium, they include audio and they have a set time limit. In this sense, the sole mention of a story

may already send a strong signal of topic salience to the audience. If the show allocates a longer time slot to the next story, then that sends the signal that the second story is even more important than the last, and so on.

The web, approached as a continuous experience produced through interactions with “relevant” information is built on what would be theoretically an “echo chamber,” each user defining his or her own agenda through content interactions. However, web architectures are not “flat;” they are designed such that certain page elements stand out more than others, certain user actions are stimulated as a result of previous actions and some sections are reserved for advertising from third parties. There are lots of opportunities to introduce historical interaction variables that will alter the “echo chamber” in favor of outside agendas—this is, after all, one of the key tasks of marketers, to introduce new “needs” that people did not even know they had. Thus, suddenly and without apparent reason, news stories and ads about political candidates start popping up on the page margins, at the top of the email inbox, in the main section of the news portal, in the home section of social networks. Take every eye contact you make with a piece of content—deliberate and accidental—convert it to time and add all intervals. This is your online political newscast.

Different media have different mechanics to accomplish the communication of salience, but what is true to all is the fact that message repetition is the most powerful indicator of topic salience to the audience. Repeating a topic day in and day out will send one unmistaken message to the public: “this is what you all need to be thinking about.” The American presidential campaign of 2016 provided plenty of examples after this pivotal moment on July 24, 2016:

> Jake Tapper: What is the reaction of the Clinton campaign to these DNC, leaked emails suggesting that top officials, including the CFO there, were actively discussing ways to hurt Bernie Sanders in the primaries?
>
> Robby Mook: Well, I think the DNC needs to look into this and take appropriate action and I'm sure that they will. *What's disturbing to us* is that we, uh...*experts are telling us* that, uh, *Russian State actors* broke into the DNC, stole these emails, and, uh, *other experts are now saying that the Russians are releasing these emails for the purpose of actually helping Donald Trump* (…) (Mook, 2016).

This “agenda-switching” move set in motion an endless—literally, it is ongoing—chain of articles and newscasts on the same topic:

July 27, 2016

a) The Washington Post, “Trump invites Russia to meddle in US the presidential race with Clinton's emails” (Rucker *et al.*, 2016);
b) The Guardian, “Donald Trump to Russia: hack and publish Hillary Clinton's 'missing' emails” (Roberts *et al.*, 2016);
c) CNBC, “Trump: I hope Russia finds ‘the 30,000 emails that are missing” (Levingston, 2016);
d) Politico, “Trump urges Russia to hack Clinton's email”(Crowley and Pager, 2016);
e) Reuters, “Trump draws ire after urging Russia to find 'missing' Clinton emails” (Holland and Stephenson, 2016);
f) The New York Times, “Donald Trump Calls on Russia to Find Hillary Clinton's Missing Emails” (Parker and Sanger, 2016a);

July 28, 2016

g) The New Yorker, “Obama’s Powerful Message: Donald Trump is Un-American” (Cassidy, 2016)
h) The New York Times, “Donald Trump’s Appeal to Russia Shocks Foreign Policy Experts”(Parker and Sanger, 2016b);
i) The Washington Post, “Donald Trump’s incredible new defense of his Russia-spying-on-Hillary comments: Just kidding!” (Blake, 2015);
j) CNN, “Democrats accuse Trump of disloyalty over Clinton emails” (Diamond and Collinson, 2016);
k) CNN, “Trump encourages Putin, America's foe” (Ghitis, 2016);

August 1, 2016

l) CNN, “Trump says Putin is 'not going to go into Ukraine,' despite Crimea” (Bradner and Wright, 2016);

August 2, 2016

m) TIME, “Donald Trump's Many, Many, Many, Many Ties to Russia” (Nesbit, 2016);

August 3, 2016

n) Politico, “Trump changed views on Ukraine after hiring Manafort” (Crowley, 2016b);

October 5, 2016

o) Mother Jones, “A History of Donald Trump's Bromance with Vladimir Putin” (Schatz, 2016);

October 12, 2016

p) Reuters, October 12, “Putin ally tells Americans: vote Trump or face nuclear war” (Osborn, 2016);

October 31, 2016

q) The Washington Post, October 31, “Harry Reid’s incendiary claim about ‘coordination’ between Donald Trump and Russia” (Blake, 2016);

November 3, 2016

r) The Washington Post, “Former CIA chief: Trump is Russia's useful fool” (Hayden, 2016);

Then, after Trump’s victory:

November 9, 2016

a) BBC News, “US election 2016: Why Russia is celebrating Trump win” (Rainsford, 2016);

November 10, 2016

b) The Washington Post, “Moscow had contacts with Trump team during campaign, Russian diplomat says” (Filipov and Roth, 2016).

When this type of metanarrative of discursive salience effectively changes the public’s perception of issue priorities (e.g., when no one discusses the Democratic Party’s undermining of Bernie Sanders to ensure the nomination of Hillary Clinton because the media does not cover the story and, instead, all they talk about is the alleged connection between Trump and Russia because that is what is on the news all the time), then the transfer of “object” salience—agenda-setting’s first dimension—has been produced. “Object” is a particularly appropriate term for the present discussion, borrowed directly from Maxwell McCombs’ terminology:

> In the abstract, the original domain of agenda setting research, an agenda of issues, is an agenda of objects. Once the agenda setting proposition has been stated in this abstract form, an agenda of objects, it becomes clear that the media can influence a wide variety of agendas. For example, our agenda of objects can be an agenda of political candidates, and there is a considerable literature supporting the view that the news media have a major voice in

> defining who are the valuable candidates for a party's nomination (McCombs, 1994, p. 175).

"Valuable candidates" are those whose attributes fit the archetype of a president. Fundamentally, in a race where one of two people will become the next president of a country, the difference between "the right candidate" and the future president should be nothing but that which turns a candidate into an authority, yet another construct. Here, I am referring to "legitimacy," which is dependent upon the continuous cultivation of collective belief in itself, according to the Weberian, rational-legal formulation of the concept (Weber, 1978, p. 213). "Belief," Habermas remind us, has no immanent relation to truth and, "if belief in legitimacy is conceived as an empirical phenomenon without an immanent relation to truth, the grounds upon which it is explicitly based have only psychological significance" (Habermas, 1992, p. 97). In a system where "the domination of society [is carried out] by 'intangible as well as tangible things'" (Debord, 1992, p. 17) this could not be more convenient for the presidential candidates who enjoy the support of the mass media system. Stabilizing a given belief in legitimacy "depends on the institutionalized prejudices and observable behavioral dispositions of the group in question" (Habermas, 1992, p. 97). Therefore, the key lies in manipulating the psycho-cognitive processes through which people form and modify their prejudices and behavioral dispositions. Defining the agenda-setting objects' attributes is the media's next contribution in this direction.

> Agenda setting is about more than issue or object salience. The news not only tells us *what to think about*; it also can tell us *how to think about it*. Bernard Cohen's classic summation of agenda setting[19]—the media may not tell us what to think, but they are stunningly successful in telling us what to think about—has been turned inside out. Both the selection of topics for the news agenda and the selection of frames for stories about those topics are powerful agenda setting roles (McCombs, 1994, p. 174).

Object attributes are conveyed to the public encoded in communication nuances afforded by the nature of medium. As their salience priorities are adopted according to the media's metanarrative, so are their attributes, which serve as cognitive semantic inputs in the public sphere's intersubjective process of knowledge construction.

---

[19] The work that Maxwell McCombs refers to is Bernard C. Cohen's "The Press and foreign policy." COHEN, B. C. The press and foreign policy. Princeton, New Jersey: Princeton University Press, 1963. 298.

However, this “knowledge” is a set of “beliefs” which the media has created the metanarrative conditions to make believe that are also “true” and “justified” (Burnyeat, 1990), hence their “knowledge” value and its “trustworthiness.” Thus, they get shared through communicative actions (Habermas, 1987); candidates start being “discursively built” into “presidents,” branded as “traitors,” or ridiculed into oblivion because, in a society in which “having” has decayed into mere “appearing” (Debord, 1992, p. 11), they don’t need to *have* any inherent qualities. What matters is to *appear*—in the right lighting and framing, on the right page, at the right hour, for however long as it is best, as many times and in as many places as possible. The media stood as the sole holder of the tools needed to create and disseminate these “legitimizable” avatars for decades with an ever-increasing power to change the tune and the beat of the public debate; “today is shall be ‘foreign policy;’ move ‘jobs’ a couple of days over in the agenda.”

Of course, this discursive orchestration is not aleatory:

> The media serve, and propagandize on behalf of, the powerful societal interests that control and finance them. The representatives of these interests have important agendas and principles that they want to advance, and they are well positioned to shape and constrain media policy (Chomsky and Herman, 2002, p. xi).

Leaving allegations of intraparty foul play aside, the overall-modest media coverage given to Bernie Sander’s promising electoral performance was atypical of a phase characterized for being covered like a horse race—lots of attention to who is leading who, a little less attention to timetables and events for the audience to look forward to, and little if any attention to policy issues (Patterson, 2016c, p. 7-8). As a result, winning candidates “appear” in the agenda more often, imbued in attributes that “explain” their victories; a metanarrative about “a candidate becoming what was meant to be.” But many things did not “unfold towards their only logical endings” in the 2016 race to the White House. Judging by the framing of Sanders as a “democratic socialist” (Ehrenfreund, 2016) or “a plain socialist” (Gross, 2016; Starr, 2016b), it was clear that his victories were not in the media’s—or the elite’s—original script. Therefore, they made sure the public got the message that, even though he was doing “surprisingly well” (Patterson, 2016c, p. 13), the idea of “him becoming the next president was unrealistic” (Dovere, 2016; Regan, 2016; Starr, 2016a; Yglesias, 2016). “No matter how you measure it, Bernie Sanders isn’t winning the Democratic primary” (Bump, 2016), “Hillary Clinton’s got this” (Enten, 2016). Accordingly, she was also getting the winner’s share of the media coverage that was being allocated to the Democratic

primaries, which was less than what the party's rivals were getting because of "the perception that Clinton had a lock on the Democratic nomination," a factor that "diminished journalists' interest in the Democratic race generally and in Sanders' candidacy particularly" (Patterson, 2016c, p. 13). However, in spite of her victories, the attributes distilled from the news stories covering her campaign did not serve to formulate the avatar of an "inevitable winner." Thomas E. Patterson argues that "the negative coverage" was a reflection of "the psychological impact" that Clinton's "worse-than-expected" performance had on the press' and the public's perception of "her inevitability." Once held as "an empirical phenomenon with an immanent relation to truth" (Habermas, 1992, p. 97), her "legitimacy potential" began to erode prematurely, it became a belief in the occurrence of a scenario that was no longer certain. But I would argue that her losses and nail-biting victories—coin flipping included—were not the causes of this; her poor performance was just an effect, not the root cause of the "negative coverage."

The narrative that made the most decisive discursive contributions to her ultimate delegitimization was the nebulous "email controversy," a story broken by The New York Times reporter Michael S. Schmidt on his article, "Hillary Clinton used personal email account at State Dept., possibly breaking rules," published on March 2, 2015 (Schmidt, 2015). But "what is found at the historical beginning of things is not the inviolable identity of their origin; it is the dissension of other things. It is disparity" (Foucault, 1977, p. 142). And this story was no exception, for it was the offspring of a series of events from which there would stem another narrative of delegitimization. Here, I am referring to a story made public by The Washington Times reporter Cheryl K. Chumley on March 19, 2013, "'Guccifer' hacker sends out Hillary Clinton's memos on Benghazi" (Chumley, 2013). Marcel Lazăr Lehel (a.k.a., "Guccifer") is a Romanian hacker who stole information from various American personalities using Russian proxy servers. Although he claimed to have no connection to Russian authorities, his preference for American political targets, as well as the geographic context from which he perpetrated the attacks provided the elements necessary to link the actions to a greater, government-sponsored conspiracy. Although Lehel would be taken into custody in January 2014, his alias and practices would be taken up by "Guccifer 2.0," responsible for the incident that Robby Mook referred to in his CNN interview (Guccifer 2.0, 2016; Mook, 2016; Nakashima, 2016b; Uchill, 2016). By then, however, the semantic connection between "Guccifer," "email" and "Russia" had had more than three years to cement in the discursive environment. Back in 2013, one of the

personalities Lehel stole information from was Sidney Blumenthal, a long-time aide of the Clintons (McLaughlin and Miller, 2015). The documents he stole where nothing less than memos with a direct connection to the U.S. House of Representatives' ongoing investigation into the attacks against the American embassy in Libya that took place on September 11, 2012. These exchanges occurred between Blumenthal and Hillary Clinton, who chose to use her private email account in the family's server, "clintonemail.com," thereby breaking the Presidential and Federal Records Act Amendments of 2014. When the State Department scrutinized Clinton's private email server as part of the ongoing congressional investigation, they realized that some of the emails that were shared were in fact supposed to be treated as "classified" information; mishandling of classified information is a crime in the U.S. (Schmidt and Apuzzo, 2015).

"Guccifer," the avatar, engendered new discursive objects that would serve as complimentary attributes to formulate the ethical dimension of the Clinton character: "Clinton's emails" and "Clinton's private email server." The former is abstract in both number and nature; the latter establishes the ownership of the former and the origin of the regulatory policies that should apply to their usage. Acting as a private citizen, Clinton was entitled to impose the rules she saw fit over the use of her own information. But acting in the capacity of Secretary of State, the preservation, storage and management of her emails are regulated by the provisions of the Presidential and Federal Records Act Amendments of 2014. Thus, the exact number of emails should have been known, their secrecy classification should have been unmistakable, and their overall creation and handling should have been conducted according to the law—not according to "private" judgment. This rendered the Clinton avatar vulnerable to the attributes that her "emails" and "email server"—discursive objects of her own making—could acquire during the course of the next 20 months.

Yet, it took much less time for the media to begin constructing the discursive bridges between the objects' circumstances and the parent avatar. Some reporters highlighted that the fact that Clinton had registered her private domain the day that her confirmation hearings for Secretary of State began before the Senate showed that "the extent of [her] hidden communication (…) is unknown" (Bump, 2015b). Others focused on the number of discrepancies found between Sidney Blumenthal's email cache and the one that Clinton turned over to the congressional committee investigating the attack on the American embassy in Benghazi, underscoring the "possible Benghazi deception

by Hillary Clinton" (Dinan, 2015). Others, focusing on the content of the emails, concluded that Clinton was "running her own rogue intel operation" (Crowley, 2015; Gerth and Biddle, 2015); "the truth may be found in her private emails." The public's reaction to these suggestive images of "secrecy as an instrument to hide foul play" can be summarized in a comment published by a user who reacted to Chumley's 2013 article on Guccifer's hacking of Blumenthal's emails: "I want to see them!!! Pretty sad that "hackers" are becoming the go to people to get the truth!" (Chumley, 2013). People holding similar views must have taken some comfort in the fact that, as The Daily Beast's reporter Shane Harris stated, "Hillary's secret email was a cyberspy's dream weapon" (Harris, 2015a).

To some a blessing, to others a curse, a year and four months after the private-email-server imbroglio hit the headlines, the second installment in the saga began: "Guccifer 2.0' claims credit for DNC hack" (Guccifer 2.0, 2016; Nakashima, 2016b). Nevertheless, this time the Democrats sought to resignify the attributes of the "Guccifer" avatar, transforming its "informational heroism"—"stealing 'the truth' from "the rich and powerful" to make it available to the bamboozled public"—into a manifestation of "Russian informational interference;" a "cyberattack on the electoral system." Controlling access to "the crime scene" was key to controlling the narrative that was to ensue around "the true identity of Guccifer 2.0." This entailed for the party to impose its will on an issue that, if indeed it was a Russian cyberattack intended to alter the outcome of the elections, it was a matter of national security—precisely the type of affair where the State is expected to exert its authority. Although it is unknown how much of a power struggle there was behind the scenes, the FBI Director James Comey's testimony before the Senate Intelligence Committee of January 2017 reveals how the Democrats managed to establish an asymmetric party-State relationship tilted in their favor. CBS News reporter Emily Schultheis covered the story:

> Comey said there were "multiple requests at different levels" for access to the Democratic servers, but that ultimately a "highly respected private company" was granted access and shared its findings with the FBI. "Ultimately what was agreed to is the private company would share with us what they saw," he said. The company to which Comey was referring is CrowdStrike, a cybersecurity company doing the internal defense and investigation for the DNC (Schultheis, 2017).

Thus, State authorities handed the Democratic Party a major political concession: the practical conditions to establish a monopoly over the empirical data necessary to attribute the attack to a particular actor. Hereafter, Guccifer 2.0's identity

could take any form the Democrats saw fit—literally, after all, CrowdStrike's client was the DNC, not the U.S.

An article published by BuzzFeed News a year after the election featured Robert Johnston, the CrowdStrike lead investigator who determined the nature and scope of the hack in the DNC's computer systems. Johnston recounted the moment when he completed and presented the findings in his diagnostic report to the Democratic Party leadership. He informed that their network "had been fully compromised" by two sets of malware from separate attacks. The oldest of the two had been operational for a whole year, while the other was only two-months old. "Both sets of malware were associated with Russian intelligence" (Leopold, 2017). Since the Democratic Party "hired CrowdStrike essentially in place of the FBI" and "Johnston was also largely on his own," the attribution of the attack was essentially based on his sole judgment (Leopold, 2017). It is worth noting that, according to the author, the article's assertions were "substantiated in interviews with 15 sources at the FBI, the DNC, and the Defense Department."

CrowdStrike's diagnosis had provided the DNC what it needed to have Guccifer 2.0's identity narrative ready by May 2016. Half way through the month, government officials started to give hints to the media. "The director of national intelligence [James R. Clapper Jr.] on Wednesday said officials had seen signs of attempted cyberattacks on 2016 presidential campaigns," reported Ellen Nakashima (Nakashima, 2016c). Yet, despite the fact that the Democrats had already identified Guccifer 2.0 as "a Russian hacker group" by then, Clapper "did not indicate whether the attempted intrusions were successful or whether they were by foreign or domestic hackers." However, other than this vague prelude, the media focused mainly on bringing their coverage of the primaries to a close. Then, on the eve of Guccifer 2.0's launch, a number of news outlets reported on the story of "the DNC hack," starting with The Washington Post:

> Russian government hackers penetrated the computer network of the Democratic National Committee and gained access to the entire database of opposition research on GOP presidential candidate Donald Trump, according to committee officials and security experts who responded to the breach (Nakashima, 2016e).

Although other outlets' headlines echoed Nakashima's assertiveness regarding the nationality of the hackers, the articles' bodies settled for more cautious affirmations. For instance, Reuters preferred to describe the intruders as, "hackers believed to be working for the Russian government" (Volz and Stephenson, 2014). Wired avoided

identifying Guccifer 2.0's nationality by referring to "two groups of hackers believed to be based in Russia" (Greenberg, 2016). The New York Times chose perhaps the most restrained approach by declaring right from the headline that the hackers' national identity was the DNC's claim: "D.N.C. Says Russian Hackers (…)" (Sanger and Corasaniti, 2016). The Guardian was equally careful by stating that the hack's connection to Russian intelligence was an allegation (Jacobs, 2016). CNN was outright distrustful:

> After the Democratic National Committee discovered it had been hacked, it made the unusual move of quickly revealing the breach to the public — including that the perpetrators were believed to be linked to the Russian government (Kopan, 2016).

But doubt did not translate into support for alternative narratives. Less than a handful of these emerged (Franceschi-Bicchierai, 2016a) and little if any attention was paid to them while they lasted (Vicens, 2016). They were nipped in the bud and quickly fell in line behind the hegemonic discursive construction project (Franceschi-Bicchierai, 2016c), which was at this point spearheaded by The Washington Post, giving visibility to the Clinton campaign's renewed efforts to substantiate their narrative—with more statements from other private contractors (Nakashima, 2016a). Nevertheless, news articles structural tendency appeared to persist throughout the campaign: headlines backing the hegemonic narrative's claims; suggestions of doubt and criticism towards the bodies' mid and bottom sections of the bodies—the places most people never reach (Pinchuk, 2016a). The New York Times was perhaps one of the few mainstream outlets to partially break with this content structure tendency (Savage and Perlroth, 2016). In the "aftermath" of the election, a lamentation that became common reading was that "the press failed the voters" for the fact that "criticism dogged Hillary Clinton at every step of the general election" (Patterson, 2016a, p. 3). I would agree with the conclusion on the basis of numerous premises—excluding Patterson's.

Sympathizing with Katrina vanden Heuvel's belief that "it is important to challenge questionable conventional wisdom and to foster debate—not police it," it seems to me that one of the media's greatest failures was that, instead of "focusing on unreported or inadequately reported issues of major importance and raising questions that are not being asked," it promoted their eclipsing (Heuvel, 2017). To me, as far as the identification of Guccifer 2.0 is concerned, Motherboard's Lorenzo Franceschi-

Bicchierai summarized what was systematically eclipsed in an idea for which he reserved the last paragraphs—precisely my point—of a 1342-word article:

> The Smoking Gun?
>
> None of this new data constitutes a smoking gun that can clearly frame Russia as the culprit behind the almost unprecedented hacking campaign that has hit the DNC and several other targets somewhat connected to the US presidential election.
>
> Almost two weeks ago, the US government took the rare step of publicly pointing the finger at the Russian government, accusing it of directing the recent string of hacks and data breaches.[20] The intelligence community declined to explain how they reached their conclusion, and it's fair to assume they have data no one else can see (Franceschi-Bicchierai, 2016b).

Without direct access to the DNC's data, the State supported the party's narrative, to the point of formally accusing Russia. This entailed not one, nor two but three "leaps of faith" on the part of American authorities: that the DNC hack was not a creation of their own; that the private contractors' assessment of the hack was not decisively influenced by their client's political interests and their own cultural and political prejudices and that Russian group of hackers had indeed a connection to the Kremlin. I would argue that the preexisting discursive conditions surrounding the objects "Putin," "Russia," and/or "hacker" provided the psycho-cognitive elements needed for the media to deliver an agenda that the public could consume as "facts" requiring no further evidence to be digested as such.

Recent "history" provided the "empirical" elements necessary to weave this belief environment, however, this "history" I am referring to is not one of historical events in and of themselves, but rather, their mediatized spectacles. To cite a few examples: "Cyber-intruder sparks response, debate" (Nakashima, 2011), "How Russian hackers stole the Nasdaq" (Riley, 2014), "The massive hack of the Nasdaq that has Wall Street terrified of cyber attacks" (Yang and Holodny, 2014), "Russian hackers use 'zero-day' to hack NATO, Ukraine in cyber-spy campaign" (Nakashima, 2014b), "Russian hackers amass over a billion Internet passwords" (Perlroth and

---

[20] Franceschi-Bicchierai refers to the Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security. See DEPARTMENT OF HOMELAND SECURITY PRESS OFFICE. **Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security**. Washington, D.C.: Department of Homeland Security Press Office, 2016.

Gelles, 2014), “Russian hackers target NATO, military secrets” (Kharpal, 2014), “Hackers breach some White House computers” (Nakashima, 2014a), “Sources: State Dept. hack the 'worst ever'” (Perez and Prokupecz, 2015b), “Hacking of government computers exposed 21.5 million people” (Davis, 2015), “How the U.S. thinks Russians hacked the White House” (Perez and Prokupecz, 2015a), “Chinese hack of US national security details revealed days after Russian hack” (Thielman, 2015), “How Russian hackers spiked the currency exchange rate” (Reisinger, 2016). After years of being bombarded with messages constructing scenarios in which “Russian hackers” have been capable of “hacking” the White House, NATO, the Pentagon, Nasdaq, the State Department or the NSA, “hacking” the DNC sounds like an easy task in a Russian hacker’s usual to-do list.

For journalists, the question was not one of “feasibility” or “plausibility,” it was about “possible motive.” In the words of CNN reporter Tal Kopan, “Why would the Russians even hack the DNC?” (Kopan, 2016). This question lingered in the media agenda even as Guccifer 2.0 breathed life into the “Crooked Hillary” character by releasing more private documents containing damning information (Rogers, 2016). While the July 5 statement by FBI Director James Comey on the investigation of Clinton’s private e-mail server yielded a “soothing” recommendation that she not be indicted despite the existence of “evidence of potential violations of the statutes regarding the handling of classified information” (Comey, 2016), it also stated that,

> With respect to potential computer intrusion by hostile actors, [the FBI] did not find direct evidence that Secretary Clinton’s personal e-mail domain, in its various configurations since 2009, was successfully hacked. But, given the nature of the system and of the actors potentially involved, we assess that we would be unlikely to see such direct evidence.

In the media, this statement was translated as “FBI: No evidence Clinton’s email was hacked by foreign powers” (DeYoung, 2016), which while may have subtracted some momentum from the “Crooked Hillary” narrative, it also undermined the narrative of “the Russian hack of the DNC.” It was almost as if the answer to the question, “Why would the Russians even hack the DNC?,” was, “probably it did not even happen; if they did not hack Clinton’s email, why would they bother to go after the DNC?” Furthermore, “given the nature of the system and of the actors potentially involved,” seeing “direct evidence” of activities carried out by “sophisticated adversaries” “would be unlikely.” Whether he did it deliberately or not, Comey’s statements casted doubt on the empirical foundations of the DNC’s narrative, including on CrowdStrike’s—or

any other private contractor's—ability to find evidence linking Russian state actors to the alleged hack.

At the time of Guccifer 2.0's first release, the question "why would Russian state actors hack the DNC?" produced answers that were circumscribed to the divulged documents; a dossier on a man with no political background (Mitchell, 2016). Journalists and analysts from all walks of life essentially rephrased the geopolitics-oriented narrative formulated by CrowdStrike's Chief Technology Officer: "Everyone around the world is trying to figure out, 'Who is Mr. Trump?' What is his foreign policy going to be? What is it going to be in relation to Russia? He's said some complimentary things about Putin. How real is that?" (Beckett, 2016). The "answer" the media would eventually stick with was already given half way through the article that broke the story on June 14. It was presented in the form of an embedded video clip titled, "Trump calls Putin 'strong,' but insists 'strong doesn't mean good,' and the caption, "Donald Trump has repeatedly called Vladimir Putin a "strong" leader, but toes a fine line on praising the Russian president" (Nakashima, 2016e). In this case, The Washington Post leveraged the Internet's organizing principle of "relevance" to have users go through a content consumption experience that would lead them to associate the narrative of the "Russian hack of the DNC" with the narrative of "the longstanding relationship of mutual appraisal between Vladimir Putin and Trump." The media had begun cultivating this narrative since before the emergence of the Guccifer 2.0 avatar (Ioffe, 2016) and continued to feed it after the first release (Foer, 2016). This prepared the discursive grounds where an accusation of "guilt by association" could seem believable and justified. Time would only make the media apply more aggressive suggestive strategies. Eventually, the media ushered in a new phase in the agenda with a new question, best exemplified in Stephen Collinson's deductive article headline: "Who wins if Vladimir Putin meddles in the U.S. election?" (Collinson, 2016).

In what Trump would later frame as an "unfortunate joke" (Duber, 2016) he provided the Democrats and the media with "the smoking gun" that had been missing. On July 27, Trump held a news conference coming on the heels of Guccifer 2.0's release of the "'HRC Defense Master Doc' outlining criticism and defense points on issues such as U.S. military intervention in Libya, the deadly 2012 Benghazi attack and the Clinton email server controversy" (Rogers, 2016). There, he uttered a statement that would haunt his candidacy and eventual-presidency: "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing. I think you will probably be

rewarded mightily by our press" (Parker and Sanger, 2016a). This line would provide the discursive basis for the construction of a "traitor Trump" avatar.

The Democratic Party found in both the media and the State two powerful allies in this discursive construction process. For instance, on July 27, NBC aired an interview with then-president Obama during which reporter Savannah Guthrie began a line of questioning about "the controversy swirling over leaked emails showing the DNC appearing to favor Hillary Clinton and a question: were the Russians behind the hack?":

> Savannah Guthrie: Do you believe the Russians are number one behind that hack and the release, and that they are actually trying to interfere with the U.S. political election?
>
> Barack Obama: Well, I think the FBI is still investigating what happened. I know that experts have attributed this to the Russians. What we do know is that Russians hack our systems, not just government systems, but private systems. But, what the motives were in terms of the leaks and all that, I can't say directly. What I do know is that Donald Trump has repeatedly expressed admiration for Vladimir Putin.
>
> Savannah Guthrie: Sounds like you are suggesting that Putin might be motivated to prefer Trump in the White House.
>
> Barack Obama: Well, I'm basing this on what Mr. Trump himself has said. And I think that Trump's got pretty favorable coverage back in Russia.
>
> Savannah Guthrie: Is it possible in your mind that the Russians would try to influence the U.S. election?
>
> Barack Obama: Anything is possible (Obama, 2016a).

It reads as a "discursive choreography" in which a reputed representative of a well-established media outlet prompts the executive branch's highest authority to subtly establish instrumental logic connections. In a minute and fifteen seconds: the FBI was set free from the burden of confirming what the DNC's "experts" had claimed; the viewers were reminded of all hacking events of the past two years; the media's narrative regarding "the mutual admiration between Trump and Putin" is referenced by a figured who enjoys the credibility that comes with his position of power; who also performed a dramatization of the reasoning that the audience needs to follow in order to arrive to the desired conclusions. Then, on the same day, CNN published two separate articles referring to Obama's remarks during the NBC interview. Jim Sciutto, Nicole Gaouette and Kevin Liptak judged "how much doubt" could be inferred from Obama's comments and provided their answer in the form of a headline: "'Little doubt' Russia behind DNC hack, US official says" (Sciutto *et al.*, 2016). Then, Liptak made a

stronger case by identifying the identities of the “US official,” “the Russian mastermind” and “the beneficiary” in a solo article published an hour later: “Obama says it's 'possible' Putin is trying to sway vote for Trump” (Liptak, 2016). On the same night, Obama delivered a systematic deconstruction of “the Trump character” in a 45-minute speech at the 2016 Democratic National Convention in Philadelphia, putting forth the argument that he did not embody the traits of what should be the archetypical U.S. president. One of the affirmations he made to substantiate this claim was that Trump “cozie[d] up to Putin,” echoing precisely the predominant topic in the media’s agenda. This would also be reused by the media as it carried forward Obama’s legitimization of Clinton and concomitant delegitimization of Trump in the following weeks (Cassidy, 2016; Crowley, 2016a; Dionne, 2016).

Trump’s “coziness” towards Putin was used as the discursive cornerstone of “the national-security dimension” of “the Trump menace.” During an interview with CNN star anchor Christiane Amanpour on July 27, ex-Secretary of Defense Leon Panetta became one of the first members of the national-security establishment to partake of the effort to construct an “unpresidentiable” Trump avatar. Amanpour prompted him to react to the “just-in” report of Trump’s public request for help to Russia in the search for “Clinton’s 30,000 missing emails.” Panetta would “interpret” the event for the viewers, emphasizing Trump’s action as “just another reflection of the fact that Donald Trump is simply not qualified to be commander-in-chief.”

> You got now a presidential candidate who is in fact asking the Russians to engage in American politics and I just think that’s beyond the pale (...) No presidential candidate who's running to be president of the United States ought to be asking a foreign country, particularly Russia, to engage in hacking or intelligence efforts to try to determine what the Democratic candidate may or may not be doing (…) candidates have to be loyal to their country and to their country alone, not to reach out to somebody like Putin and Russia, and try to engage them in an effort to try to, in effect, conduct a conspiracy against another party [this is] just a reflection of the irresponsibility of Donald Trump. He doesn’t have the experience, he doesn’t understand the world that we live in, he’s very careless with his words (…) I think just his words alone have created a tremendous amount of damage for the United States abroad (…) This is the first election in my lifetime where there is only one candidate who has the experience, the qualities, the understanding of our role in the world that is running for president (…) she’s running against somebody who is totally unqualified, that has no experience, that has no sense of America’s role in the world (…) for anyone who is concerned about protecting our national security and (…) the defense of the United States of America there really is no choice here, Hillary Clinton is the only responsible candidate running for president of the United States (Panetta, 2016).

Later, CNN’s Jeremy Diamond and Stephen Collinson wrote an article to further propel Panetta’s criticisms and have the keywords be indexed by search engines. They

framed the ex-Secretary of State's opinion as part of a mediatic strategy on the part of the Democrats to cease Trump's careless remarks. They seemed to suggest this would go down as a decisive point in the campaign:

> Trump's comments marked an extraordinary moment in a presidential campaign that has already overturned political convention. Clinton's campaign reacted swiftly, seeking to use Trump's comments to play into their larger narrative that the Republican nominee lacks the knowledge and temperament to commander in chief (Diamond and Collinson, 2016).

"'Treason'? Critics savage Trump over Russia hack comments" (Toosi and Kim, 2016), "Former Obama mentor: Trump's Russian hack 'jokes' could 'constitute treason'" (Kelly, 2016), "Donald Trump's Appeal to Russia Shocks Foreign Policy Experts" (Parker and Sanger, 2016b), "Trump encourages Putin, America's foe" (Ghitis, 2016). The Democrats wanted to deal a devastating blow before the end of the summer. Two weeks later, 50 G.O.P. members of the national-security establishment would join Panetta's "warning" of a Trump presidency, appealing to essentially the same type of arguments used by the Democrats in a collective letter pledging to abstain from voting for Trump in spite of their party affiliation. Although rather vaguely, their closing paragraph would come to summarize the rationale that compelled millions to cast their ballots in Trump's favor:

> We understand that many Americans are profoundly frustrated with the federal government and its inability to solve pressing domestic and international problems. We also know that many have doubts about Hillary Clinton, as do many of us. But Donald Trump is not the answer to America's daunting challenges and to this crucial election. We are convinced that in the Oval Office, he would be the most reckless President in American history (Hayden *et al.*, 2016).

Accused of treason, deemed politically incompetent and with no shortage of scandals concerning a wide variety of issues: from associations with mafia figures, to sexism, racism and xenophobia. How would a candidate so "unpresidential" survive the overwhelming and relentless attack of the alliance between the Democratic Party, the State and the media, and come out as the winner of the electoral contest despite his record? It seems to me that McCombs' conceptualization of the agenda-setting process is elucidating in this regard:

> In the abstract, the original domain of agenda-setting research, an agenda of issues, is an agenda of objects. Once the agenda-setting proposition has been stated in this abstract form, an agenda of objects, it becomes clear that the media can influence a wide variety of agendas (McCombs, 1994, p. 175).

McCombs' formulation of the abstract dimension of agenda-setting seems to imply that what is understood as "the agenda-setting function of the media"—the production and transfer of discursive objects and attributes to influence the public's perception of the world through the organization of the conditions for communicative action—is not immanently contingent upon the media institutions in and of themselves. The dissemination of information subsidies such as videos, speech transcripts, photos and emails may influence both the content of the "news" and the public's perception of the environment (Turk, 1985; 1986; Kiousis *et al.*, 2009; Kiousis and Strömbäck, 2010; Marland, 2012). Therefore, any agent capable of divulging these types of subsidies, transmitting a narrative of objects and attributes, and generating a metanarrative of object salience that an audience incorporates as a guide to "knowing what is relevant" has the potential to perform the agenda-setting function that has been historically owned by the media (Parmelee, 2013). In fact, as an agenda-setting entity, such agent has the potential to influence how the media shape their own agenda. For this to take place, however, there ought to exist a communicational context of trust. On the one hand, this is contingent upon the audience's perception of both the agent proposing the agenda and the medium in which the messages are exchanged. On the other hand, it also depends on the extent to which the experience of the messages' qualities invokes their rationalization as "possibly accurate" representations of "facts" in the minds of the message receivers.

By the same token, failure to produce the basic conditions for the articulation of a communicational context of trust may result in the hindering of the capacity to effectively perform the agenda-setting function. As explained earlier in this chapter, whether it be in the message transfer process from the media institutions to the public, from a person to another, or from a person to a larger group, audience trust lies at the heart of agenda-setting. It is key in the construction of beliefs that are assimilated as truthful representations of facts in the physical world, even without being directly confirmed through individual empirical testing. Therefore, provided that a communicational entity enjoys or is capable of producing conditions of trust for the transfer of "belief-seeding" messages between itself and the audience, the agent may have the potential to generate a sustained belief-construction relationship with the audience whose trust it enjoys. As belief is also based on the individual's and society's preconception of what is possible—established through a combination of rationalization and empirical experience—the capacity to produce messages

integrating “believable” semblances of past, present and future “real-life” objects and scenarios is utmost important to the stimulation of audience-based belief construction. In an age of spectacles, the one capable of producing “believable” mirages in a context of communicational trust may have the power to condition how an audience sees the environment after which the mirages are built.

In the context of a political campaign where mainstream media has sided with one of the candidates, the rival at a disadvantage may seek to foster the construction of beliefs that can result in the corrosion of the public trust in the media. This may result in undermining not just the credibility of both the media and his opponent, but also their capacity to effectively manage the public’s belief-construction—or, for all practical purposes, their capacity to exercise their agenda-setting function. Furthermore, as actions are based upon beliefs, and conditioning the latter subsequently conditions the former, making the public distrust the media and the candidate who they seek to benefit may also succeed in turning the public into a protective body against their attacks and overall criticism.

If messages such as “the media are a bunch of liars” (Smith, 2016; Talbot, 2016) or “forget the press, read the Internet, study other things, don't go for the mainstream media” (Trump, 2016) are delivered over a context of trust, the audience may very well cease to trust the media and get their news from social media. Statistics indicate that this is precisely what happened. The Pew Research Center’s “News use across social media platforms 2016” report published towards the end of the Republican primaries showed an increasing reliance on social media as a source of news among adults (Gottfried and Shearer, 2016). Furthermore, Edelman’s “Trust and the U.S. presidential election” report also showed that, by the time the 2016 American presidential election had come to an end, media trust had suffered one of the fastest and steepest declines in history (Edelman, 2017). Thus, messages such as, “our country is going to hell” (Wojnowski, 2016) are delivered over a communicational context of trust, that is, from a trusted source over a trusted medium, may cause the audience living in such country to internalize this perception as “the real state of affairs.” Simultaneously, the public may also distrust their president when in his televised speech he claims that “after the worst recession in 80 years, (…) deficits [came] down, 401(k)s [recovered], [the] auto industry set new records, unemployment [reached] eight-year lows, and (…) businesses [created] 15 million new jobs” (Obama, 2016c).

Trump was a figure who enjoyed audience trust in the realm believed to be “a source of news” by a majority; social media. In this realm, he portrayed their tripartite alliance, constructing a narrative of conspiracy: “the Establishment’s conspiracy against the underdog candidate.”

> FBI documents reveal just how deep the corruption goes. The undersecretary of state, Patrick Kennedy, illegally pressured the FBI to unclassify e-mails from Hillary Clinton's illegal server.
>
> It's hard to believe. And nothing happens to her, folks, and nothing ever happens. In other words, the State Department was trying to cover up Hillary's crime of sending classified information on a server our enemies could easily access.
>
> The FBI document shows that Patrick Kennedy made the request for altering classification as part of a very, very serious quid pro quo. Not allowed to do it. This is a felony corruption. Yesterday, I said Undersecretary Kennedy must immediately resign.
>
> The media barely covers this event, by the way.
>
> This is a bigger event than Watergate and they practically refuse to cover it. Today, I'm calling for him to be fired (Trump, 2016).

Thus, when, for instance, the HuffPost called Trump—the trusted agent—“a serial liar, rampant xenophobe, racist, misogynist, birther and bully” (Mazza, 2016), or when Slate ridiculed him as “Putin’s puppet” (Foer, 2016), the attacks were not only dismissed as “lies” from “liars [who] will be sued when the election is over” (Bierman, 2016), they also served to prove Trump’s point that he was being the victim of a defamation campaign involving a tripartite alliance among the Democrats, the State and the media. This is precisely what shielded Trump’s avatar from their attacks and supported his claim that he was “the authentic outsider candidate” being attacked by the Establishment (Boykoff and Laschever, 2011; Berlet, 2012). The “authenticity” quality of this “outsiderness” was reinforced not only by Trump’s heavy reliance on social media channels to disseminate his ideas regardless of the editorial media’s planned agenda, but also on the seemingly “amateurish” quality of many of the subsidies his campaign and supporters mediatized through the Internet. In contrast, Clinton’s digital marketing assets and overall messages appeared to be produced by professional communicators or otherwise “professionalized” marketing efforts (Enli, 2017). As this also played into the narrative of “the politically-correct candidate,” the Trump campaign constructed it as a trait reminiscent of the notion of “more of the same”—a recreation which Trump constructed as a negative scenario (Rebuilding America Now, 2016; Conway *et al.*, 2017).

It is worth noting that Trump's opponents created the conditions under which his conspiratorial narrative proposing an alliance between the Democrats, the State and the media met standards of plausibility: the State allowed the DNC to keep control over the empirical evidence substantiating the narrative that Guccifer 2.0 was an invention of Russian State actors (Comey, 2017), later ratified the Democrats' discourse through the formal condemnation of Russia as the mastermind of the DNC hack without having directly analyzed the source of the alleged evidence (Binney *et al.*, 2017; Comey, 2017), and the media served the role of constructing a narrative in which talks of evidence took the place of actual evidence and allegations took the place of facts (Johnson, 2016; Comey, 2017). This alone would have sufficed, yet the content of the hacked emails also reinforced his narrative. CNN feeding debate questions to Donna Brazile in advance (De la O, 2017); Debbie Wasserman Schultz demanding apologies from MSNBC host Mika Brzezinski for criticizing her bias against Bernie Sanders (Norton, 2016); and Politico's Maggie Haberman being listed as a "friendly journalist" who has "never disappointed" in the Democrats' leaked "media strategy document" (Greenwald and Fang, 2018) are just a few examples of controversies that made headlines during the campaign.

Back when the media had the monopoly over the means of mass communication, inflicting such crisis of trust in the media may have been nearly impossible. However, ICTs provided the technology for both the development of conditions of trust and the construction of messages articulating "believable" semblances of "real-life" (Rose, 2015). This diffused the power to exercise the agenda-setting function that had been historically monopolized by the media institutions, providing the public with the tools to effectively influence their networked audiences (Chadwick and Stromer-Galley, 2016; Chadwick, 2017; Waisbord *et al.*, 2018). Therefore, the degree of accessibility of these communicational capabilities supposes a challenge to the media's power to condition the candidates' attributes and the issues that the public should regard as "most important" when defining their competence, credibility, authenticity and overall trustworthiness. This raises the question of whether it would be in the media's best interest to support their candidate by giving less attention or altogether ignoring the subsidies shared by her political opponents.

The technological and communicational mechanisms propelling the communicational processes that result in interpersonal and multi-personal influencing are also the ones that drive the monetization of the data and information exchanges

on which the Internet economy is based (Ramer *et al.*, 2009a; Perler, 2012; Najjar and Kettinger, 2013). Therefore, the interests that tend to prevail in the mass media institutions decision-making processes pertaining to the control of these societal influencing dynamics are those that align with their stimulation, rather than their curtailment (Solomon, 2018). The monetization of web content, on the other hand, is driven by users' interaction with visual elements that draw explicit and implicit user input; systems register these interactions and use the data to refine the personalization and microtargeting of messages (Barocas, 2012; Barbu, 2014; Borgesius *et al.*, 2018); the mechanism that shortens the path from message visualization to monetizing events. It is therefore in the media's profit-making interests to give visibility to the pieces of content that stimulate these interactions, for even if they do not lead to direct purchases, they generate the data needed for the systems to calibrate their targeting and increase the profitability of their outreach.

Approached from this holistic perspective, the monetization process itself values interactions from supporters of both candidates alike and, as private enterprises' ultimate goal is to generate and multiply capital and profit for their shareholders, this is also the prevailing logic for mass media corporations (Berkowitz, 1993; Coddington, 2015; Haeg, 2018; Alterman, 2019). They may despise one candidate or another but reducing visibility of the content they find engaging based on conflicting political affinities ultimately goes against the media enterprises' existential principle. And, in an age of spectacle, "scandal politics" are the audience's favorite; easy to "digest," highly entertaining and, as such, highly profitable (Castells, 2009).

This is why the media simply could not resist covering Trump's speeches and events, or his supporters' controversial views and behaviors: they sold well (Somaiya, 2015; Crovitz, 2016; Elving, 2016). They may have manifested, disseminated and evoked the expression of values that run contrary to the American Establishment's moral discourse and the imaginary on which they based their Nation-State project. Yet, at the same time, the mediatization of such dramatizations was as purposeful to the generation of capital as infotainment and "confrontainment" (Boorstin, 1992; Lloyd and Friedland, 2016; Ouellette, 2016; Podkalicka *et al.*, 2018). In the end, the hunt for profitable, trending, sensationalist content took over the search for candidates' communicative actions (Patterson, 2016b), which, in the case of Clinton, were the discursive manifestation of her strongest suits. Therefore, key issues such as how she planned to bring to bear her experience to the materialization of her government plan

became much less visible than the attributes constituting the “unpresidentiable” dimension of her character (Google Trends, 2016). Both the media and the public could have switched this equation around, but scandal seemed to draw more attention than academic and professional preparedness—arenas in which Clinton had a clear advantage over Trump.

Moreover, in a race between a candidate who is already portrayed as “a man of scandal” even prior to entering the contest, and another who seeks to stand at the higher moral ground of the archetypical “experienced statesperson,” the latter is the one who stands to lose the most in a mediatic environment permeated by scandal and controversy. This is because her legitimation is contingent upon the prominence given to her positive attributes in the mediatized construction of her character. But people search for “dirt” and “drama” (Google Trends, 2016), therefore, the media has a greater incentive to give them the “takedowns,” the “comebacks,” the “secret recordings” and the “confidential emails.” Thus, in practice, the profitability of scandal politics exacerbated the premature erosion of Clinton’s legitimacy, while the entertaining nature of Trump’s avatar inoculated him from the effects of the scandals swirling about him.

At no point did Trump seek to compete with Clinton on the claim to be “the most presidential of candidates” (Obeidallah, 2016). In fact, he seemed to drop the idea of competing on an explicit or tacit claim to having a pristine record or a flawless character. Quite the opposite; he sought to capitalize on his imperfections to epitomize “the simple, matter-of-fact outsider who made his billions through ‘real’ work—not politics.” Concomitantly, he created a narrative of a country that was brought to the verge of disaster by “the Washington Establishment,” a group in which he also included the core of the Republican Party. This helped him validate his claim to being the only outsider in the race. Then, his discourse legitimized the free expression of discontent against the institutions and groups that he claimed to embody the existential threat to “real American values” and “the American way of life.” These expressions of discontent led to chaotic dramatizations of anger, fear and strife. Instantly mediatized on all corners of the U.S., “the country going to hell” that he forecasted was there for all to see. Prophet of a self-fulfilled prophecy, he then presented himself as “the American messiah,” “the scourge of the Establishment” and “their job-killing, anti-American policies,” “champion” against immigrant “terrorists,” “thieves” and “rapists,” “the only one who can bring about a new social order of justice for real Americans.” He

constructed a new “presidentiable” archetype based on an alter reality that he, too, constructed; an archetype whose mold he and no one else could fit in.

The media play the central role of providing the stage where the avatars are constructed; these constructs are “real” insofar as they are believed to be “true” representations of the “real-world” entities they reference. If, on the contrary, the “grand spectacle” they depict is seen as “fake,” their constituting messages cease to bring about the psycho-cognitive effects that produce the continuous adoption of the media discourse as the priority and meaning of reality (Tandoc *et al.*, 2018). With the media’s collaboration, the Democrats sought to “wake the public up” from “the Trump spectacle” by priming the Russian intervention narrative on the news; the story of how he was nothing but “an unwitting agent of Russia,” as asserted by former deputy CIA Director Michael Morell in an opinion piece published by The New York Times on August 5, 2019 (Gass, 2016; Morell, 2016). Thus, they imbued the narrative with “objectivity” by having “American State actors” respond to the aggressions allegedly perpetuated by “Russian State actors,” for this is the political outcome that they “would have probably” produced had the purported intervention occurred in a scenario of “undeniable factuality.” However, the diplomatic approach they chose for the dramatization of these actions was one that contextualized the responses in the discursive realm in which the electoral battle was unfolding, that is, as instantly mediatized actions that everyone could see. This was no accident; the electorate needed to witness the avatars of statesmen doing “what statesmen do in the face of foreign interference.” How else could the public believe that they were indeed certain of the veracity of the Democrats’ claim?

On July 30, The Daily Beast’s Michael Crowley published an article echoing the concerns of members of the national-security Establishment such as William J. Perry, Secretary of Defense under Bill Clinton, warning that the “campaign rhetoric aimed at discrediting Trump, may be taking on a life of its own, making global problems harder to solve and increasing the risk of an accidental conflict — potentially even a nuclear one” (Crowley, 2016a). According to Perry, “we’re sleepwalking into a new Cold War (…) there’s hardly any debate about it, and the public doesn’t understand the danger.” This is in part due to its failure to comprehend how “the global scope and speed of [ICT-driven] communication” have vested in “small groups at the pinnacle of political and economic structures [the power] to process and monitor information, shape debate, and to some extent define truth” (Kissinger, 2014, p. 356). Key distinctions to

the exercise of policy-making have become blurred: “between information, knowledge, and wisdom, (…) between domestic and international upheavals, and between leaders and the immediate demands of the most vocal groups.” Expected to respond to “events whose effects once would have taken months to unfold [and now] ricochet globally within seconds,” authorities are tempted “to cater to the demands of the digitally reflected multitude.” This leads to hasty political actions guided more by “the mood of the moment” evoked by the instrumental narratives of a few, than by “the judgment required to chart a complex course in harmony with long-term purposes.”

> Leadership (…) risks being reduced to a series of slogans designed to capture immediate short-term approbation. Foreign policy is in danger of turning into a subdivision of domestic politics instead of an exercise in shaping the future. If the major countries conduct their policies in this manner internally, their relations on the international stage will suffer concomitant distortions. The search for perspective may well be replaced by a hardening of differences, statesmanship by posturing. As diplomacy is transformed into gestures geared toward passions, the search for equilibrium risks giving way to a testing of limits (Kissinger, 2014, p. 358).

While Crowley’s article may have delivered a somewhat appeasing hint to the Russians—“at the moment, the Obama administration’s top worry is not nuclear war but ending the Syrian civil war [which] many U.S. officials believe (…) can only be settled with Russian assistance”—the tone of the narrative was much less reassuring elsewhere in the media. It went from legal scholars with ties to reputable institutions such as Yale and Harvard discussing whether domestic and international cyberlaw would rule the hacking of the DNC as an instance of “election interference” (Goldsmith, 2016; Velde, 2016), to journalists questioning if such “cyber interference” could be considered “cyberwarfare” and hence, an “act of war” (Chotiner, 2016; Jordan, 2016; Szoldra, 2016). Mediatized discussions using this type of rhetoric went on for months, setting the stage for rhetorical reaction from a person whose position gave his statements the weight of an official threat made by the U.S. against Russia.

WikiLeaks’ release of the so-called “Podesta emails” on October 7 marked a pivotal point in the State’s direct commitment to the Democrats’ narrative as it triggered a formal accusation against “Russia's senior-most officials” made through a joint statement from the Department of Homeland Security and the Office of the Director of National Intelligence on Election Security (Department of Homeland Security Press Office, 2016). This would be the first in a series of discursive actions from the U.S. intelligence community supporting the idea that “the thefts and disclosures [were] intended to interfere with the US election process” and that “it was in a position to

attribute this activity to the Russian Government." Then, on October 14, then-vice-president Joe Biden upped the ante during an interview on NBC's "Meet The Press." In response to a question loaded with allegations presented as facts, Biden made a statement that would further raise the political stakes: "We're sending a message. We have the capacity to do it. It will be at the time of our choosing, and under the circumstances that will have the greatest impact" (Biden, 2016). Complementing Biden's declaration, NBC published an article which affirmed that, "the Obama administration [was] contemplating an unprecedented cyber covert action against Russia in retaliation for alleged Russian interference in the American presidential election" (Arkin et al., 2016). Other media outlets did their part in assuring that at least NBC's content would indeed have "the greatest impact" possible (Snyder, 2016; Tacopino, 2016).

Initially, Biden's statement and the dozen mediatic warnings of a purportedly "imminent non-conventional attack" that followed it raised concerns among high-ranking Russian officials (Bridge, 2016; Simonyan, 2016a). Nevertheless, in the end Putin did not see Biden's bet; he shrugged off his comments while reiterating that Russia had nothing to do with any of the hacking activities that his administration was being accused of carrying out (Pinchuk, 2016b; Simonyan, 2016b). This still did not convince then-president Obama. On December 28, 2016, he signed an executive order establishing a state of "national emergency with respect to significant malicious cyber-enabled activities" (United States, 2015, p. 1), defining the content, scale and reach of the provisions for retaliatory action. In practice, the latter is limited to the economic and diplomatic realms (United States, 2015, p. 1-3) and are intended to be targeted to the individuals, institutions, enterprises or States that the Secretary of the Treasury, the Attorney General and the Secretary of State may accuse as "aggressors" (Codevilla, 2018);. To be sure, they took the heaviest toll on American-Russian diplomatic relations since the end of the Cold War, judging by the response of Vladimir Putin's Press Secretary (Roth and Filipov, 2016).

The following day, Obama gave a press conference at the White House in which he reaffirmed both his belief that "based on uniform intelligence assessments, the Russians were responsible for hacking the DNC, as well as his interest in reviewing all elements [to prevent] that kind of interference through cyber-attacks in the future" (Obama, 2016b). To that effect, he proceeded to recapitulate "how this thing unfolded," as he put it. His explanation was, however, a criticism to the press he was addressing

at the conference, whom he seemed to suggest was a collective actor and not just a mere spectator of the events:

> Let's just go through the facts pretty quickly. At the beginning of the summer, we were alerted to the possibility that the DNC had been hacked and I immediately ordered law enforcement, as well as our intelligence teams to find out everything about it, investigate it thoroughly, to brief the potential victims of this hacking, to brief on a bi-partisan basis the leaders of both the House and the Senate and the relevant intelligence committees. Once we had clarity and certainty around what in fact had happened, we publicly announced that, in fact, Russia had hacked into the DNC. At the time we did not attribute motives, or any interpretations of why they had done so. We didn't discuss what the effects of it might be. We simply let people know (…)—just as we had let members of Congress know—that this had happened. And, as a consequence, all of you wrote a lot of stories about (…) what had happened and then you interpreted why that might have happened, and what effect it was gonna have in the election outcomes—we did not (Obama, 2016b).

Over the course of the following two years, it would become clear that the purpose of Obama's final actions as a sitting president went beyond blaming the media for "misinterpreting" acting State officials' numerous suggestions that they stood by CrowdStrike's attribution of the alleged hack. Through the expansion of economic and diplomatic sanctions, Obama could not have been realistically hoping to accomplish much more than the modest impact that had been achieved since 2014, when the U.S. and the E.U. imposed their first set of sanctions to pressure Russia to withdraw from the Crimean Peninsula. The Graduate Institute Geneva's Targeted Sanctions Consortium analysis of the usage of sanctions by the UN is elucidating in this respect. According to Nataliia Slobodian and Iryna Ptasnyk, "on average, sanctions are effective in achieving their stated goals approximately 31 percent of the time (…) ultimately [being] more effective at signaling or constraining than eliciting a change in behavior" (Slobodian and Ptasnyk, 2018). On the one hand, this is due in part to the fact that not all EU countries perceive Russia as a threat in the same way—or at all. "Nord Stream 2 has allowed the Kremlin to expand its export capacity to the EU and circumvent the Baltic states, Poland, Slovakia, the Czech Republic, and Ukraine – giving Moscow a stronger hand in its Eastern European policy;" Germany, France and Austria have lobbied in favor of this. In fact, the lack of consensus appears to extend to the U.S.-E.U. dyad, with several European countries accepting the American initiative only for a limited period of time and remaining skeptical of Washington's efforts to arm Ukraine as a means to bring stability to the region. Furthermore, Russia counts with powerful Asian allies whose commercial exchanges are bound to weaken

the effects of American sanctions, chief among them, China and India. Therefore, it should come as no surprise that “the actual potential of sanctions to change or moderate Russian behavior” has been relatively low from the start. Enacting them, however, does serve a purpose much closer to home: creating a policy that, given its punishing nature, continuously gives “objectivity” to the claim that it was “Russian State actors” that commanded the hacking of the DNC. However, it was utmost important that the enactment of such policy was undoubtedly born out of the rationale of the State’s national security and not the vengeance of the Democratic Party. This is the reason why it was crucial for Obama to complete the imposition of the sanctions prior to the end of his term, while reestablishing the purported impartiality of the State and tacitly affirming the objectivity of the Democrats’ assessment of the information leak that jeopardized Clinton’s run for the presidency. Thereafter, lifting the sanctions would have been a sign of “friendliness towards the enemy;” a sign of treason.

But, to what extent was the Washington Establishment truly concerned about Rand Waltzman’s “Russian Threat”? Almost as in an act of foreshadowing, on May 9, 2016, Senator Mike Rounds introduced a bill titled, “Cyber Act of War Act of 2016,” a bill “to require the President to develop a policy for determining when an action carried out in cyberspace constitutes an act of war against the United States, and for other purposes” (United States, 2016a). On May 12, Representative James A. Himes introduced a similar bill in his chamber (United States, 2016b). Neither bill made it too far: Rounds’ was “read twice and referred to the Committee on Foreign Relations,” while Himes’ was “referred to the Subcommittee on Emerging Threats and Capabilities.” For a country that had been the target of several Russian hacking attacks since 2014, this anemic response to concrete legislative attempts to reach clarity about what constitutes a “cyberattack” and the type that may warrant going to war seemed awfully contradictory. This contradiction was only comparable to the vehement attempt of the American delegation at the June 2017 meeting of the UN Group of Governmental Experts (UN GGE) to have the report on the international regulation of cyberspace contain provisions for “the potential applicability of the right to self-defense and the general international law principles of countermeasures” (Henriksen, 2019, p. 3).

> In a statement issued after the unsuccessful discussions were concluded, the Cuban representative stated that he was concerned with “the pretension of some . . . to convert cyberspace into a theater of military operations and to legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs”. He objected to statements in the draft report that

> in his mind sought to “establish equivalence between the malicious use of ICTs and the concept of “armed attack . . . which attempts to justify the alleged applicability in this context of the right to self-defense”. Allegedly, this constituted a “fatal blow to the collective security and peacekeeping architecture established in the Charter of the United Nations”, essentially turning the field into a “Law of the Jungle”, in “which the interests of the most powerful States would always prevail to the detriment of the most vulnerable”. The Cuban representative also highlighted the draft report’s references to the law of armed conflict because it “would legitimize a scenario of war and military actions in the context of ICT” (Henriksen, 2019, p. 3)

The Cuban delegate’s statements seemed asynchronous with his country’s and its allies’ posture in July 2015. Then, much alike the rest of the report’s contributors, Cuba, Russia and China expressed a common understanding on the issue of the applicability of the provisions of the UN Charter to the governance of cyberspace. More precisely, they accepted “the inherent right of States to take measures consistent with international law and as recognized in the Charter,” of which the right to self-defense is, of course, an integral part. Discursively, Russia’s stance in 2017 appeared to imply that the country had strong reasons to oppose accountability and punishment for infractions to international law on the cyber domain. This is because, in 2015, Russia’s position entailed the assumption of both the obligations underlying the application of international law on cyberspace activities and, in the event of failure, the corresponding penalties. Thus, Russia had concurred "that existing obligations under international law are applicable to State uses of ICTs," including the "nonintervention in the internal affairs of other States; (…) that States have jurisdiction over the ICT infrastructure located within their territory,” that States are obligated by international law “not to ‘use proxies to commit internationally wrongful acts using ICTs’ and to ‘ensure that their territory is not used by non-State actors to commit such acts’.” Therefore, even if the Cuba-China-Russia trifecta’s stance was nothing more than a strategic move following the notion that the “less powerful States always try to use norms and legal interpretations to try to ‘level the playing field’” (Henriksen, 2019, p. 5), given the predominant discursive environment marked by the globally mediatized narrative of “the Russian hacking of the 2016 U.S. presidential election,” Russia’s decision to withdraw from its previous posture seemed to provide “further proof that the U.S. has been correct all along” in accusing Russia. After all, their understanding of international law in 2017 appeared to suggest that they did act in contradiction to their previous interpretations, they just did not want to be held accountable for their actions.

> In reaction to the June 2017 UN GGE disappointment, the American representative noted that the US had come to the “unfortunate conclusion that

> those who are unwilling to affirm the applicability of these international legal rules and principles believe their states are free to act in or through cyberspace to achieve their political ends with no limit on their actions" and that this is "a dangerous and unsupportable view" (Henriksen, 2019, p. 5)

In the end, however, this led to nothing more than the conditions necessary for the American representative to make the exposition above. Once again, the U.S. could not be realistically expecting anything different from Russia given the discursive climate it had created the previous year. Much like the economic sanctions imposed by Obama at the end of his term, the American participation in the UN GGE of 2017 had no real punishment as its ultimate goal. Rather, it seems to me that the objective was to create a scenario that would force the Russians to take a diplomatic course of action that would be instrumental to the American narrative attributing the hacking of the DNC to their country.

But, if the measures taken at home and abroad were not wholeheartedly aimed at forcing Russia to abstain from orchestrating "interferences" similar to the one that they allegedly carried out in 2016, what did the U.S. hope to accomplish with their symbolic diplomatic actions? With a Trump administration now in full swing, "replaying" the narrative of the Russian hack into the DNC could only have a transcendental effect in the advancement of the narrative with which the Democrats sought to prematurely delegitimatize candidate Trump. It is also the same narrative that has accompanied him over the course of his first term as president of the U.S.: the narrative of "the Russian collusion," or "Russiagate," as it has come to be called (Boyd-Barrett, 2018).

Although it grew during the campaign, the post-election period has seen not merely a replay of previous media events. Even before Trump was sworn into office, the media began enriching the "Russian hack" narrative, interweaving old and new artefacts for its rearticulation as an outcome of the influence of Putin's personal vision in the trajectory of post-Soviet Russia and its overarching objectives (Kirk and Wiser, 2017). This exercise in "historical reconstruction" has been executed according to a grand metanarrative structure linking previously unrelated objects, appearances and scenarios, thereby producing a more cohesive, linear and "easily-digestible" story. On June 7, 2018, PBS NewsHour published a vista of this metanarrative: "The giant timeline of everything Russia, Trump and the investigations" (Desjardins, 2018).

As a portal to a universe of articles published on major mainstream media channels about events that occurred sometime between 1998 and the present, PBS'

“giant timeline of everything Russia” is a metaphor representative of the news industry’s prolonged, relentless effort to “flesh out” the “Traitor Trump” character. Structured by news topic (e.g., “Major Events,” “Investigations,” “Russians Hacking” and “Trump”), this Google Spreadsheet is a “large and well-meaning” map (Foucault, 1977, p. 140) plotting all the “facts and historical events”—all the media stories, rather—necessary for the (re)construction of a discursive puzzle that, no matter the starting point, conveniently ends in the portrayal of the same inescapable conclusion: “the president is the latest of Putin’s pawns in his vengeful crusade against Clinton, the U.S. and the West.”

The publication of many of the media artefacts comprising this narrative followed soon after the historical events they make references to. First, “Crimean parliament seized by unknown pro-Russian gunmen” (Salem *et al.*, 2014), then, the first of Obama’s sanctions against Russia: “Executive Order 13660: Blocking property of certain persons contributing to the situation in Ukraine” (United States, 2014a), “Executive Order 13661: Blocking property of additional persons contributing to the situation in Ukraine” (United States, 2014b). Then came the Russian response: “Sources: State Dept. hack the 'worst ever'” (Perez and Prokupecz, 2015b). Almost concomitantly, the Obama administration further increased the pressure over Russia: “Russia is ousted from group of 8 by U.S. and Allies” (Smale and Shear, 2014), “Executive Order 13694: Blocking the property of certain persons engaging in significant malicious cyber-enabled activities” (United States, 2015). Russia replied in kind: “How the U.S. thinks Russians hacked the White House” (Perez and Prokupecz, 2015a). A request was issued: “Obama to Putin: Stop Hacking Me” (Harris, 2015b). Putin replied: “Russia hacks Pentagon computers: NBC, citing sources” (Kube and Miklaszewski, 2015). PBS’ “timeline” also includes more recent articles that fill in “historical gaps;” stories about events that allegedly occurred but were not covered when they “happened”: “New details emerge about 2014 Russian hack of the State Department: It was ‘hand to hand combat’” (Nakashima, 2016d), “Russian hackers stole U.S. cyber secrets from NSA [in 2015]: Media reports” (Volz and Menn, 2017), “Obama tried to give Zuckerberg a wake-up call over fake news on Facebook” (Entous *et al.*, 2017). The map is a resource maintained by dedicated and thoughtful investigative journalists trying to help colleagues and readers around the world “connect the dots.” As such, it reflects mainstream media’s agenda-setting roadmap.

Of course, some of the “dots” being connected also refer to new efforts to delegitimize the president. From a January 2017 Intelligence Council Assessment (ICA) that, without presenting a shred of evidence

> assess with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election, the consistent goals of which were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency (…) Putin and the Russian Government aspired to help President-elect Trump’s election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him (Office of the Director of National Intelligence, 2017, p. ii).

Thereafter, the news could justifiably claim that “Vladimir Putin intervened in [the] U.S. election to help Donald Trump win” (Schulberg, 2017), while stigmatizing “those less willing to take the intelligence assessment on faith” (Graham, 2017). Thus, anyone who was not satisfied with the Office of the Director of National Intelligence’s failure to explain the methods used to arrive to the report’s conclusions risked being labeled a “conspiracy theorist,” much like the DNC did when scolding The Nation magazine for publishing Patrick Lawrence’s article, “A new report raises big questions about last year’s DNC hack” (Lawrence, 2017):

> U.S. intelligence agencies have concluded the Russian government hacked the DNC in an attempt to interfere in the election. Any suggestion otherwise is false and is just another conspiracy theory like those pushed by Trump and his administration. It’s unfortunate that The Nation has decided to join the conspiracy theorists to push this narrative.

But the Democrats were anything but alone in pushing their narrative. The 2017 ICA’s attribution of the alleged DNC hack to Putin himself was further reinforced by Special Counsel Robert S. Mueller’s federal indictment of thirteen Russian citizens for “supporting the presidential campaign of then-candidate Donald J. Trump (“Trump Campaign”) and disparaging Hillary Clinton” (Washington, 2018a). Although The New York Times preferred to report Mueller’s work as “a sprawling indictment that unveiled a sophisticated network designed to subvert the 2016 election and to support the Trump campaign” (Apuzzo and LaFraniere, 2016). David Corn, Mother Jones’ Washington bureau chief and an on-air analyst for MSNBC, took Mueller’s “stunning indictment” and resignified it: “the special counsel’s charges reinforce what we already know: Trump aided an attack on America (…) [this is an indictment of] President Donald Trump and his Republican minions” (Corn, 2018). Needless to say, this rhetoric mirrored the function of the headlines eager to find an empirical support—no matter how feeble—to claim the existence of a quid pro quo agreement between Putin and

Trump back in early July 2016. To this effect, adding to the 2017 ICA and the indictment of the so-called “Internet Research Agency,” Mueller would deliver yet a second indictment, this time against twelve members of Russia’s Main Directorate of the General Staff of the Armed Forces (G.U.) who

> used the Guccifer 2.0 persona to release (…) stolen documents through a website maintained by an organization (…) that had previously posted documents stolen from U.S. persons, entities, and the U.S. government (…) [and] continued their U.S. election-interference operations through in or around November 2016 (…). To hide their connections to Russia and the Russian government, the Conspirators used false identities and made false statements about their identities. To further avoid detection, the Conspirators used a network of computers located across the world, including in the United States, and paid for this infrastructure using cryptocurrency (Washington, 2018b).

Although different from CrowdStrike’s report regarding the timeline of events, it was the first time in two years that an American official issued a coherent, detailed and plausible explanation that could support what had been claimed and instrumentalized to aid one presidential candidate and handicap another. Although still considered allegations, not proofs, Mueller’s statements even describe the building in central Moscow where the group was hacking the DNC from, the tactics the hackers used and the methods that the investigators utilized to develop the findings contained in the indictment. The media could not be happier. It further cemented the idea that what they had been selling the public as “facts” for the previous two years was indeed true. Better yet, it, too, was bound to sell:

> It’s always on Fridays. Almost like clockwork, each new indictment from the Special Counsel’s office released on a Friday afternoon, just in time to disrupt the weekend news cycle. Not that anyone is complaining, because this week’s indictment is a blockbuster—an 11-count indictment of 12 Russian military officers alleging that they engaged in a hacking campaign against Hillary Clinton, the Democratic National Committee and the Democratic Congressional Campaign Committee (Rosenzweig, 2018).

With a meeting between Putin and Trump a few days away, “the timing of the newest indictment in the special counsel's Russia investigation couldn't be better for President Trump's opponents,” as Amber Phillips noted (Phillips, 2018). The media was going through what seemed a moment of joy. Paul Rosenzweig’s optimism was emblematic: “with the special counsel’s latest indictment, Americans are one step closer to knowing the truth of what happened during the 2016 election” (Rosenzweig,

2018). With or without the G.U. officers standing trial in the U.S.—the likelihood of which is minimal, given that it would require Putin's approval— "the truth" that the media has been after has not changed since July 2016: Trump's role in the operation.

Brewington et al. provided one of the most complete explanations of how Mueller's second indictment "move[d] the ball forward on possible collusion" (Brewington *et al.*, 2016). Their article also contained a characteristic that would become increasingly common in the media environment after Mueller released his final report: the signaling of possibility in the absence of explicit contradiction.

> While the document does not allege any American who corresponded with these entities knew that they were part of the Russian conspiracy, it also does not say that they did *not* know or suspect these entities were part of a Russian operation. It leaves that question, about these actors and others, for another day (…) In other words, stay tuned. This indictment represents a tightening of the ring in the story of criminal prosecution for the 2016 election hacking. The government has now alleged that the social media manipulations by Russian actors constituted a criminal conspiracy. It has alleged as well that the hacking of Democratic Party and Clinton campaign emails were crimes conducted by officers of the Russian state. The question remains: Who, if anyone, helped? (Brewington *et al.*, 2016)

The media built the Mueller investigation into the source that would provide the empirical event on which to found a set of beliefs that would devastate Trump's legitimacy; the grounds for impeachment (Habermas, 1992). As for the Democrats, some even went as far as to say that he became a sort of "folk hero amid the Russia investigation" (Associated Press, 2019). Indeed, they felt such strong confidence that their two-year investment was going to yield the political returns they had been longing for that on March 14, 2019, the House of Representatives—where the Democrats currently hold majority control—voted 420-0 to release the Mueller report to the public. Mueller submitted his final report to Attorney General William Barr on March 22. Barr and his team reviewed the document and created a summary which he made public on March 24. "A total exoneration!" Trump claimed Mueller's final report amounted to (Karamehmedovic, 2019). Nonetheless, the media were quick to deny him a full victory:

> The investigation led by Robert S. Mueller III found no evidence that President Trump or any of his aides coordinated with the Russian government's 2016 election interference (…) However, (…) Mr. Mueller's report states that "while this report does not conclude that the president committed a crime, it also does not exonerate him" on the obstruction of justice issue (Mazzetti and Benner, 2019).

> Regardless of what Robert Mueller's report contains, Americans can draw comfort from the fact that the special counsel completed it. In spite of numerous attempts by Donald Trump to interfere with Mr Mueller's

> investigations — including at least two occasions where he reportedly tried to fire him (…) the story is far from over (Financial Times Editorial Board, 2019).

And the story does seem to be far from over, for as House Intelligence Chairman Adam Schiff said even before Barr handed his disappointing report summary, "impeachment is still possible even if Russia probe clears Trump" (Oprysko, 2019). Thus, once again, one narrative dies providing the seeds for the next. So much time was spent trying to prove that Trump committed some form of treason that all the players have reached the next campaign cycle. And this is precisely the Democrats' new strategy. On March 11, Speaker of the House of Representatives Nancy Pelosi made it clear that they will not pursue Trump's impeachment (Heim, 2019). Yet, Democrat candidates Kamala Harris, Elizabeth Warren, Pete Buttigieg are actively demanding Congress to proceed with the impeachment process, while other candidates are saying that "voters can impeach Trump at the ballot box in 2020" (Stolberg and Fandos, 2019). In the end, the latter is perhaps the most transparent of slogans, for this is what they all know that is realistically accomplishable with the statements from the Mueller report that have been made public thus far. In essence, their claim is that, "as is," the report portrays an "impeachable" president who is therefore an "unpresidentiable" candidate.

However, the Democrats' two-year investment has so far backfired and the political scenario that best illustrates this is the upshot of the fight over funding for Trump's southern wall project. This is because of its symbolic connection to both the discursive construction of his legitimacy in his way to the presidency and the nature and goals of the policy proposals that have been successfully blocked by federal judges since he became president of the U.S. The southern wall construction project was discursive constructed as "the solution" to a series of "existential threats to 'real' Americans" posed by what Trump characterized with epithets such as "drug traffickers," "criminals" and "rapists." Hence, just as it is a symbol of the electoral support that this securitizing discourse garnered him, the project's deliverable—the wall—is the material proof that he made his legitimized mandate effective. On the other hand, as "the keeper of White-American safety," the southern wall project is the epitome of the racist and xenophobic ideology that Trump articulated in both his campaign speeches and his administration's agenda. At the same time, the discursive traces of this ideological platform have provided sufficient legal evidence for federal judges to block much of Trump's "national security" agenda, thereby effectively

curtailing his capacity to deliver on the promises he made as part of his securitization campaign (Denniston, 2017; Barbash *et al.*, 2019).[21] The federal rulings that blocked Executive Orders 13769 and 13780 (i.e., "Protecting the Nation from Foreign Terrorist Entry into the United States") are elucidating in this regard. In June 2017, Judge Derrick K. Watson presiding the United States Court of Appeals for the Ninth Circuit ruled:

> The President's authority is subject to certain statutory and constitutional restraints. We conclude that the President, in issuing the Executive Order, exceeded the scope of the authority delegated to him by Congress. In suspending the entry of more than 180 million nationals from six countries, suspending the entry of all refugees, and reducing the cap on the admission of refugees from 110,000 to 50,000 for the 2017 fiscal year, the President did not meet the essential precondition to exercising his delegated authority: The President must make a sufficient finding that the entry of these classes of people would be "detrimental to the interests of the United States." Further, the Order runs afoul of other provisions of the INA [Immigration and Nationality Act] that prohibit nationality-based discrimination and require the President to follow a specific process when setting the annual cap on the admission of refugees (Washington, 2017, p. 2-3).

Trump came back three months later with Order 13780. Watson, however, had a similar answer:

> [The Executive Order] suffers from precisely the same maladies as its predecessor: it lacks sufficient findings that the entry of more than 150 million nationals from six specified countries would be "detrimental to the interests of the United States," a precondition that the Ninth Circuit determined must be satisfied before the Executive may properly invoke Section 1182(f). Hawaii,859 F.3d at 774. And [the Executive Order] plainly discriminates based on nationality in the manner that the Ninth Circuit has found antithetical to both Section 1152(a) and the founding principles of this Nation. Hawaii, 859 F.3d at 776–79 (Hawaii, 2017, p. 2).

Trump's "Protecting the Nation from Foreign Terrorist Entry into the United States" Executive Orders were as emblematic of his overarching racist and xenophobic immigration agenda as they were of his failure to utilize the legitimate authority granted by the audiences that voted for him based on the promise to exercise his power to defend them from "the threats" he constructed in his securitization discourse. Blocking the construction of the southern wall had been a major setback for the same reasons, but it was being carried out through different legal mechanisms. Up until late March of

[21] It should come as no surprise that Trump is reconfiguring the ideological composition of the judiciary system by appointing judges that he believes will be more likely to uphold his orders. Past presidents have done this in one way or another, but none of them rival the pace of Trump's initiative. See MARIMOW, A. E. **Two years in, Trump's appeals court confirmations at a historic high point**. The Washington Post. Washington, D.C.: Fred Ryan 2019.

this year, the project had been prevented by Trump's detractors at both ends of the political spectrum in the House of Representatives and the Senate, who had done so by continuously excluding Trump's $5.7 billion request for the wall's construction from the federal budget. The battle came to a head when Trump tried to force the hand of Congress by subjected the federal government to what would eventually become its longest shut down in history. With 71% of Americans considering the wall "not worth the shutdown" (Salvanto *et al.*, 2019) and 53% of Americans blaming him and his party for the shutdown (The Washington Post and ABC News, 2019), Trump began to see his overall approval ratings decline (Clement and Nakamura, 2019). In response to this, Trump suspended the shutdown with the intention of "resuming negotiations over the funding of the wall," yet legislators from both parties agreed to a bill that approved a federal budget that ignored Trump's $5.7-billion request. On February 15, Trump responded by issuing Proclamation 9844, a declaration of national emergency:

> The current situation at the southern border presents a border security and humanitarian crisis that threatens core national security interests and constitutes a national emergency. The southern border is a major entry point for criminals, gang members, and illicit narcotics. The problem of large-scale unlawful migration through the southern border is long-standing, and despite the executive branch's exercise of existing statutory authorities, the situation has worsened in certain respects in recent years (...) Because of the gravity of the current emergency situation, it is necessary for the Armed Forces to provide additional support to address the crisis (...) NOW, THEREFORE, I, DONALD J. TRUMP, by the authority vested in me by the Constitution and the laws of the United States of America, including sections 201 and 301 of the National Emergencies Act (50 U.S.C. 1601 *et seq.*), hereby declare that a national emergency exists at the southern border of the United States, and that section 12302 of title 10, United States Code, is invoked and made available, according to its terms, to the Secretaries of the military departments concerned, subject to the direction of the Secretary of Defense in the case of the Secretaries of the Army, Navy, and Air Force. To provide additional authority to the Department of Defense to support the Federal Government's response to the emergency at the southern border, I hereby declare that this emergency requires use of the Armed Forces and, in accordance with section 301 of the National Emergencies Act (50 U.S.C. 1631), that the construction authority provided in section 2808 of title 10, United States Code, is invoked and made available, according to its terms, to the Secretary of Defense and, at the discretion of the Secretary of Defense, to the Secretaries of the military departments (Trump, 2019).

Thus, through an act of securitization, Trump planned to circumvent Congress' express disapproval of his most salient piece of security policy, invoking the emergency powers contemplated in the National Emergency Act (United States, 1976), more specifically, the provisions laid out in section 2808, the "Construction authority in the event of a declaration of war or national emergency":

> In the event of a declaration of war or the declaration by the President of a national emergency in accordance with the National Emergencies Act (50 U.S.C. 1601 et seq.) that requires use of the armed forces, the Secretary of Defense, without regard to any other provision of law, may undertake military construction projects, and may authorize the Secretaries of the military departments to undertake military construction projects, not otherwise authorized by law that are necessary to support such use of the armed forces. Such projects may be undertaken only within the total amount of funds that have been appropriated for military construction, including funds appropriated for family housing, that have not been obligated (United States, 1982).

Nevertheless, the law on national emergency proclamations allows for their legislative overturning by approving a privileged resolution by simple majority vote in both chambers of Congress. On February 26, the House of Representatives passed a joint resolution stating that "the national emergency declared by the finding of the President on February 15, 2019, in Proclamation 9844 (84 Fed. Reg. 4949) is hereby terminated" (United States, 2019). By March 14 the Republican-majority Senate had followed suit. On March 18, as expected, Trump vetoed the resolution. Trump's opposition also expected to have the two-third majority votes in both the House and the Senate that it would require to override Trump's veto. This would have effectively defunded his wall construction project. Yet, before the House was able to reconvene to deal the final blow, Mueller completed his report and Barr made his summary public.

Suddenly, a president whose legitimacy had been consistently questioned since before he sat foot in the White House and effectively blocked since he became president was reinvigorated by the power of public perception. To some, a "total exoneration" entailed that Trump's claims that the investigation was nothing more than a partisan "witch hunt" perhaps deserved some credibility after all. Even Pelosi, who had voiced her disapproval of the idea of impeaching Trump, seemed to catch a breath with Barr's summary, for it seemed to erode any possible legal basis that could justify such uncertain pursuit. As for the veto override, on March 26, two days after the "Russiagate" shipwreck began to unfold on everyone's screens, the Democrats were unable to gather the votes they needed to complete the two-third majority in the chamber they lead.

Noam Chomsky summarized the Democrat drama of the past two years in an interview with Amy Goodman, reporter from Democracy Now!,: "The Democrats invested everything in ["Russiagate"]. Well, turned out there was nothing much there. They gave Trump a huge gift. In fact, they may have handed him the next election" (Goodman, 2019). Democrats sought to destroy the legitimacy of an authoritarian,

charismatic politician by exploiting sheer rumor. In the end, when an official investigation produced “the closest thing to knowledge of the matter,” their opportunistic claims managed the exact opposite of what they intended. Not only did they legitimize him, they were also unable to prevent the consummation of an authoritarian act: the imposition of a major national construction project according in a “one-way-or-another” fashion. Imagining history being written according to Chomsky’s fears, one cannot help to recall one of Karl Marx’s most famous reflections as he set out to critique the conditions that permitted Napoleon III to put an end to the French Republic and put France back on the path of imperialism: “Hegel says somewhere that that great historic facts and personages recur twice. He forgot to add: ‘Once as tragedy, and again as farce’” (Marx, 2009, p. 1).

Though I doubt Trump would be able to make a habit of exploiting the opportunistic crusades of the Washington elite to legitimize the advancement of the authoritarian agenda he set out to accomplish as president, the reader and I shall find out soon enough whether Americans are in for a second taste of the farce—a coalition of the media, the Democratic Party and the State paving the way for Trump’s second term as they try to delegitimize him with unsubstantiated allegations. Luckily, farce did not turn into tragedy in July 2016, when the dramatization of rumor as proven fact led high-ranking officials to play dangerous parts in a scenario constructed with the conceptual building blocks found in the “information warfare” discursive framework. At the same time, the crisis appeared to have exposed the effects of decades of inconsistencies and incongruencies between and among the framework’s concepts, applications and discursive manifestations (Lord, 1989).

Late Senator John McCain was one of the most vocal elements of the American military Establishment to express his profound concern. During an interview he gave to the "1+1" Ukrainian TV channel on December 30, 2016, he began addressing one of the “basic cyber questions that [the] nation has yet to answer”: “What constitutes an act of war or aggression in cyberspace that would merit a military response, be it by cyber or other means? (McCain, 2017)”

> There are many sanctions we can take. Financial institutions, for one. Believe it or not, the Russians have a very weak economy; we could do a lot more damage there. Individuals could be sanctioned; organizations could be sanctioned. There is a wide range of options that we still have of additional options that could be exercised to respond to a Russian attack. When you attack a country, it is an act of war, and so, we have to make sure that there is a price to pay, so that we can perhaps persuade the Russians to stop this kind of attacks on our very fundamentals of democracy (McCain, 2016).

The following day, Reuters published a poorly-edited cut of the interview along with an equally abridged audio transcript. It barely mentioned any references to nonmilitary retaliatory measures and highlighted that “John McCain said (…) that Russia must be made to pay the price for cyber attacks on the United States (…) ‘When you attack a country, it's an act of war,’ McCain said (…) ‘And so we have to make sure that there is a price to pay (…)’” (Karazy and Williams, 2016; McCain, 2016). Also on New Year’s Eve, CNN’s Theodore Schleifer and Deirdre Walsh published an article referencing Reuters’ audio transcript of McCain’s interview. They titled their article, “McCain: Russian cyberintrusions an 'act of war'” (Schleifer and Walsh, 2016) and they reported that, “Sen. John McCain said Friday that Russia’s alleged meddling in the 2016 presidential election amounted to an ‘act of war.’” Thus, what was originally expressed as one in a series of nonbelligerent forms of retaliatory action for cyber deterrence purposes was constructed as the discourse of the

> Chairman of the Senate Armed Services Committee (…) [who has also] scheduled a hearing for next week on foreign cyberthreats to the US (…) [and] Russian cyberhacking, (…) who is one of Washington's most prominent foreign policy hardliners, has criticized the recent sanctions and expulsions announced by the Obama administration this week as insufficient and belated (Schleifer and Walsh, 2016).

Schleifer’s and Walsh’s characterization of McCain does not correspond to the avatar in the interview aired on the Ukrainian channel. Per their portrayal, McCain appears to be “the hardliner” who not only has the power to influence the U.S. to opt for engaging in warfare against Russia to the detriment of “softer” retaliation tactics, but has also made up his mind about “exacting revenge.” The reporters ignored his interest in developing a clear cyber security framework—one of the main purposes of the hearings that would follow five days from then—and, judging their article strictly on the interview they referenced, they lied about his criticisms in regards to “the recent sanctions,” which McCain explicitly included among “the wide range of options” available to persuade Russians to stop their attacks.

The reporters’ misrepresentative characterization of McCain and his discourse finds a rationale in the fact that both the prospect of violence as well as the fear and anxiety it creates among audiences sell more than the possibility of settling disputes through diplomatic efforts. And though Russian intelligence is likely aware of these mediatic profitability practices, there is simply no infallible method that can guarantee

actors' accurate reading of the political scenario before them, nor would a correct reading necessarily conduct to "logical" reactions on their part. Moreover, even if Russian intelligence were to engage in the type of compare-and-contrast exercises that shed light on the media's manipulation attempts, it is uncertain whether the decision-makers' cultural and ideological biases could have a greater weight in their view of the scenario. Back in December 2016, all that the general audience saw was John McCain—indeed an influential policymaker and a leader in the American security apparatus—saying, "Russia," "cyberintrusions" —a term not even mentioned in Reuters transcript—"act of war," "make sure that there is a price to pay." Since McCain was portrayed as "a hardliner," the audience was led to imagine that "the price" in question was probably meant to be "paid in lives." What did the General Staff of the Armed Forces of Russia see? If the Russians' reading of the then-chairman of the Senate Armed Services Committee depended on Reuters' and CNN's reporting of his interview in Kiev, they could have easily believed that, given McCain's position and influence, the U.S. was moving towards the execution of some type of military retaliation. If beliefs guide actions, then Putin could have placed Russia on war footing. Once there, there is no telling what may light the fuse. This is precisely one of the main reasons why having a framework including definitions of cyber offenses, standards of attribution, measures of retribution and overall rules of engagement is necessary.

Such was the overarching objective of the series of Senate Armed Services Committee hearings that were scheduled to begin less than a week later: to address the American cybersecurity policy dilemma. McCain would preside over the first of the hearings, which he introduced as a review whose "goal [was] not to question the outcome of the presidential election. Nor should it be. As both President Obama and President-elect Trump have said, our Nation must move forward. But we must do so with full knowledge of the facts (...)." Up to this point, McCain's discourse appeared to adopt a nonpartisan, purportedly "fact-based" stance similar to Obama's in his December 16 press conference (Obama, 2016b). This changed as soon as he claimed to possess "knowledge" of "Russian interference in [the] recent election" based on the "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security" of October 7, 2016 (Department of Homeland Security Press Office, 2016):

> We know a lot already. In October, our intelligence agencies concluded unanimously that, quote, the Russian Government directed compromises of emails from U.S. persons and institutions, including from U.S. political

> organizations. They also assessed that, quote, disclosures of alleged hacked emails were consistent with the methods and motivations of Russian-directed efforts and that these thefts and disclosures were intended to interfere with the U.S. election process (McCain, 2017, p. 4).

Thereafter, McCain's intervention—and the subsequent review process—became partisan, for it was circumscribed to what the Democrats had claimed to be "knowledge" about the alleged hacking of their computer systems. Although the joint DHS-ODNI statement's odd combination of "confidence" and "belief" when referring to the claim "that the Russian Government directed the recent compromises of e-mails from US persons and institutions" should have sufficed for McCain to reconsider the trust he conferred to the statement, just five days later, FBI Director Comey would declare under oath that the FBI had not been granted access to the DNC's computer systems. This by itself would undermine any claims to "knowledge" made by the U.S. Intelligence Community (USIC)—the signatory of the statement that McCain based the review's initial assumptions on. Even then, the Senate Armed Services Committee's hearings of the following months would all take Russia's antagonistic role as a given and departure point. One of these hearings took place on April 27, 2017. Then, Rand Waltzman gave the testimony that introduced the topic of this dissertation, which, as analyzed, was not the exception—it put forth the idea that to confront "the Russian threat" it is necessary to conduct a continuous countrywide cyber-psycho-cognitive operation (Waltzman, 2017). And I would contend that the hearings were themselves part of Waltzman's "cognitive security" project. The work of "answering pressing cyber questions" became intertwined with that of characterizing Putin and Russia as immanent adversaries of the U.S. such that, whoever gets associated with them becomes vilified too—the newly-elected president being first in the list.

> What seems clear is that our adversaries have reached a common conclusion: that the reward for attacking America in cyberspace outweighs the risk. For years, cyber attacks on our Nation have been met with indecision and inaction. Our Nation has no policy and thus no strategy for cyber deterrence. This appearance of weakness has been provocative to our adversaries who have attacked us again and again with growing severity. Unless we demonstrate that the costs of attacking the United States outweigh the perceived benefits, these cyber attacks will only grow. This is also true beyond the cyber domain. It should not surprise us that Vladimir Putin would think he could launch increasingly severe cyber attacks against our Nation when he has paid little price for invading Ukraine, annexing Crimea, subverting democratic values and institutions across Europe, and of course, helping Bashar Assad slaughter civilians in Syria for more than a year with impunity (…) Put simply, we cannot achieve cyber deterrence without restoring the credibility of U.S. deterrence more broadly (McCain, 2017, p. 5).

But insofar as this type of rhetoric did not bring about the tragedy of war, it simply kept feeding the farce of building an ever-worse foe to portray and ever-worse traitor. Waltzman, however, deserves credit for articulating a whole new function for the "Russian threat" narrative: legitimizing domestic cyber-psycho-cognitive operations. To be clear: they were already happening, but now they will be carried out as part of the American national security doctrine, hidden in plain sight. Waltzman's "cognitive security" prescribes the integration of a series of triple-helix elements that has in fact been operational for quite some time. The lead-up to the American presidential election of 2016 saw such machinery at work. It was the power struggle between two candidates using ICT-based resources and mechanisms for the sake of exerting dominance over the discursive definition of the other. Each portrayed the other as part of a political narrative that not merely polluted the public's perception. While providing the elements for the articulation of beliefs instrumental to the construction of the other as "an unpresidentiable candidate," both Clinton and Trump planted the seeds for the premature and utter erosion of legitimate authority. Though with different degrees of success, both candidates leveraged neural networks' deep learning computational capabilities to systematically evoke visceral emotional reactions at the encounter of the rival's attributes. It seems to me that the one who provided the most subsidies to substantiate his narratives' claims prevailed in the electoral struggle—which, as we now know, was not the end; it was just the start of a new chapter. Although the election produced one delegitimized politician who has spent the better part of the past two years hiding from the public eye, the actors and forces that drove her campaign's cyber-psycho-cognitive operation have continued their attempt to delegitimize the now-president of the U.S. They have been so perseverant in their effort that they are heading into the new campaign cycle using an advanced stage of the same narrative they were using as their presidential train derailed in 2016.

5. CONCLUSION

At the abstract level, cyber-psycho-cognitive operations are prolonged mediatized processes through which microtargeted audiences are guided through the construction of lifeworlds using discursive frameworks that make the formation of certain strategic beliefs and political outcomes more probable. Cyber-psycho-cognitive operations bear similarities to traditional military psychological operations, yet their instrumentality goes beyond military actors and purposes. Using the theory, practice and discourse of information warfare as a point of departure, this research found that there is a wide range of political actors capable of wielding them as instruments for political destabilization. And this is their core function: to induce legitimation crises through the modification of aspiring or ruling authorities' primed attributes in such a way that the public perceives them as embodying roles in political narratives that society could hardly bring itself to either support or continue supporting. While this may result in dangerous power vacuums, the process of reaching the legitimation crisis can also engender other risks to national security, including internal sociopolitical turmoil. In this sense, through the articulation of specific and conflicting ideational contexts, cyber-psycho-cognitive operations can "weaponize" a country's own population against itself, triggering processes of mutual destruction among domestic social groups.

To do this, cyber-psycho-cognitive operators leverage the "relevance" and "authority" principles on which the web's organizing mechanisms are based, creating content and content relationships that make elements of the discursive frameworks of interest more predominant in agents' lifeworlds. Then, as the "relevance" principle makes content recommendation engines serve objects (e.g., ads, profiles of people you may want to follow, profiles of people you may know, sponsored comments, events, groups, pages, apps, etc.) that are somehow "related" to the lifeworlds' predominant discursive frameworks, agents are hardly ever—or never—exposed to the possibility of engaging in communicative action with agents who either share similar experiences but have validly different perceptions of "reality," or experience life in different contexts but share similar perceptions of "reality." Thus, agents become "trapped" in lifeworlds of programmatic "similarities" and their socialization produces cohesive, "knowledge-based" tribes. When the individual and group interests

stemming from these tribal nuclei face off in a public consultation scenario where the outcome grants the winning side the power to impose conditions that the losing side perceives as immanently incompatible and unacceptable according to their lifeworlds, the political choice ceases to be a conflict between and among interests that can be conciliated through negotiation and becomes an existential battle—that is, in the narrative about the consultation and in the minds of those "living" it. Then these "knowledge-based" tribes may feel compelled to engage in open confrontation.

At the heart of the phenomenon studied in this dissertation lies the belief on which the construction of these lifeworlds is based, synthetized by Guy Debord long before the start of the ICT revolution. People became so accustomed to both "representing" the world around them and presenting their "representations" as "narrative placeholders" of the physical environment, that objects ceased to possess the quality of "having" attributes. Now, they just "appear" to have them, for most experiences are not encounters with the objects themselves but rather, with their representations. And yet, the inherent indirectness of these representations seems to have no effect in their ascribed "factuality;" makers and beholders alike count "factuality," "objectivity" and "impartiality" among their potential properties. Hence, representations are treated as perfectly-valid, knowledge-building materials in day-to-day life. This would not be conducive to an eased propagation of false information if all representations had to pass through the same rigorous scrutiny that scientific sources do before they can be considered "knowledge sources." But, in fact, ICTs have only made it increasingly easy to both construct and disseminate immersive, interactive information user experiences that play out like seamless dialogues between individuals and systems that "always seem to know what they want." Powered with deep-learning artificial intelligence, these systems engage users with "the most relevant, context-based, information responses." These semantic experiences are calculated constructions integrating the web's dynamically-evolving content inventory according to person- and cohort-based, user-information interaction tendencies recorded in a myriad real-life scenarios. This is both a curse and a blessing.

For the same reason that a 36-year-old man is likely to see an Amazon.com shopping ad for a yellow shirt right after he watches a full one-minute-long, Tommy Hilfiger video advertising the shirt's entire collection on YouTube, an engine may have recommended for him to read an article titled, "WikiLeaks confirms Hillary sold weapons to ISIS … Then drops another bombshell," if sometime after August 4, 2016

he happened to read about how Hillary Clinton's State Department approved weapon shipments to Libya during the uprising against Muammar Gaddafi in 2011. Although the article's actual impact in the election results is unknown, BuzzFeed reported that it accrued a total of 789,000 engagements before November 8, 2016 (Ritchie, 2016). How many of these users spread the "news" as "facts"? How did these "facts" echo other ongoing narratives designed to construct an "unlegitimizable" avatar spectacle? How many people propagated the article's misinformation as "facts" without even providing its URL to their audiences? And how many of these people believed the information without questioning its veracity because they trusted the source?

Make no mistake; fundamentally, the phenomenon that I have dissected in this dissertation does not begin and end with the truthfulness of information. It does not boil down to how "perfectly 'presidentiable' political candidates can be prevented from becoming presidents as a result of 'fake news' shared through social media," as Clinton herself would have you believe (Clinton, 2017). Rather, the focus should be on how the practice of ICT-enabled communication has led to a dependency on the automatization of information prosumption processes, including the acceptance of instantly-mediatized narratives' validity, accuracy and truthfulness. Whether "truthful" or "fake," the knowledge economy requires for users to operate with the metaphors produced by ICTs as if they trusted that their functionalities and the qualities of their outcomes will remain the same regardless of time and space.

When it comes to news-related avatars, the expectation is that their function as providers of reliable information will be trusted every time. For instance, a moving image of Anderson Cooper appearing on a screen over a blue background, accompanied of a red CNN logo on the left-hand lower corner, or a news article with the words, "by Ellen Nakashima," typed right under its title and over a white-background web page with "The Washington Post logo" should both automatically persuade the message receiver to believe that the oral and written expressions presented through the media are representative of the people behind the avatars. Accordingly, they should be given the trust and credibility they and their channels have earned after years of performing the same functions and outputting the same outcomes. Decision-makers from all spheres of social activity follow suit, as does everyone following their leadership for one reason or another; thus, trust in the validity of the narratives as direct representations of real entities and phenomena becomes a norm of the utmost importance to sociopolitical and economic life.

But once the norm has been incorporated as a behavior enabling the capacity to perform without questioning the "factuality" of the narratives, it has become programmed as a characteristic in the relationship between the agent and the online media. Then, if ICTs allow for the simultaneous creation and sharing of space-time-compressed narratives containing all the symbols necessary to build and elicit audience trust and credibility, the message receivers simply apply the programmed behavior for the reception of such type of narratives and proceed to trust in the information transmitted as if it was "factual" just because it is being conveyed over the programmed dynamic. Furthermore, for anyone with a desire to be economically active in the informational society, the incorporation of this program is not an option. In this sense, it structurates agents to have a bias towards trusting the realm of online information as a reliable source of narratives. The potential psycho-cognitive effects that these narratives can have in a political candidate's image, or in the stability of a country's overall political system is independent from whether the "news" are "real" or "fake."

The glocalized American party politics and foreign policy power struggles of the last two years have been telling in this regard. The 2016 presidential campaign neatly revealed a global phenomenon driven by ICT platforms' capabilities to engage in emotionally-arousing, individualized dialogues. This is thanks to their continuously-improving deep-learning algorithms and their increasingly enhanced capacities to seize the expanding learning opportunities emerging from users' information prosumption activities. Furthermore, the private ownership of these platforms and their central role in all spheres of social activity have made both the deep-learning algorithms' capabilities and users' data available for rent. Since becoming platform clients in 2008, the 2016 election was the first time that user-emotion-aware machine recommendations were leveraged to deliver political narratives at the times that they could cause the greatest impact to a person that fit a particular profile. Moreover, their capacity to programmatically and strategically select and construct each of the messages interwoven in the narratives was also instrumental to the driving of users along specific belief-construction journeys and, therefore, to the advancement of candidates' political strategies whose main goal seemed to revolve around the undermining of the opponent's path to becoming "legitimizable." Given recommendation engines' recursive logic, the microtargeting of audiences with discourses that put forth such type of "reality scenarios" led to the articulation of

“knowledge-based” tribes. The effects of these narratives and their development dynamics were bound to have profound effects beyond the election, especially in terms of the degree of social polarization they brought about.

However, this dissertation did not analyze how online social discourse reflected the societal effects of these narratives. Though critical to the completion of a theory on cyber-psycho-cognitive operations, such endeavor was unattainable with the knowledge and skills that were available at the time of research. Instead, it focused on studying the phenomenon’s trajectory, first, by characterizing it according to the discursive paradigm at the moment when a panel of qualified experts and decision-makers formally articulated its existence as a security vulnerability and, second, by discovering some of the “discursive trace evidence” it left as it manifested through artefacts produced by the media, the political parties and State officials. With the goal of developing an understanding of the “security vulnerability’s” nature and dimension that could be detached from mediatic sensationalism, this exploration began by inquiring into the conditions of possibility for preventing future cyber-psycho-cognitive operations from happening, given its propelling forces. At this point in the analysis, the assumption was that, if economic disincentives could be introduced either in the psycho-social processes of narrative articulation, or in the production of some of the materials that are critical for the execution of these processes, the phenomenon would cease to have the means to manifest itself as an effective threat.

This analytical quest required revisiting Moore’s Law (Moore, 1965), which laid the foundation to explain the material origins of the inverse relationship between, on the one hand, microprocessors’ decreasing sizes and prices, and, on the other, their exponentially increasing computational capacity. Historical economic trends corroborated the validity of the forecasts that emerged from the application of Moore’s principles. As time moved forward, computers became smaller and their processing power vastly superior. This processing power led to faster innovation and the production of more groundbreaking advances, which further accelerated innovation processes, including those that derived in the design and development of smaller and more powerful computing devices. Shortly after hardware began its exponential improvement cycle, innovators such as Douglas Engelbart started devising mechanisms with which people could access processors’ computational capacities regardless of their technical skills (Engelbart, 1962). This signal the start of the user-computer interface and, tacitly, through the execution of repetitive input motions and

the triggering of predictable behavioral outcomes, the cognitive foundations for computer-mediated narrative construction were laid. Physical and Graphic User Interfaces helped realize the economic potential underlying the continuous production of smaller devices at lower costs: the incorporation of computers into all dimensions of social activity could begin. Thus, the making of narratives grew along with the dramatization of user-computer communication dynamics; the rise of the Internet helped evolved the dyad into computer-mediated multi-user communication. As ICTs' sizes eventually allowed for their total mobility and the infrastructure supporting the Internet allowed to be accessible from any location, narratives became increasingly contextual. Moreover, advances in data production, storage, handling, enrichment and distribution would further exploit computers' processing capacities, putting them on the road towards communicational independence from humans. Contextual narratives could be articulated in real-time collaboration, not just between users, but also between users and machines powered with artificial intelligence. The private ownership of both the hard and soft infrastructure that supports these interactions marks their end goal: profit-making. Even though, users' daily interactions with information are as seamless as they are effortless, they produce one of the most valuable commodities of our time: unstructured and semi-structured, enriched data. It all seems "free" and gamified; data prosumption does not seem to be as hard as a regular nine-to-five job, but it is highly profitable for those who own the means to capture and sell the data. Thus, an entire new economy has grown. It is based on machines registering, storing and passing data combinations including semantic expressions and contextual signals to inform digital property owners what the users in their markets are interested in and to calculate the messages that they need to be exposed to in order to accomplish their business objectives. As time goes by, the infrastructure, the know-how and the need to engage in this growing economy are only being enhanced. If stalling cyber-psycho-cognitive operations depended on the erosion of this economy's pillars, it is hard to see how preventing another event like the 2016 American presidential election could be possible. In fact, provided that there is an interest on the part of the actors capable of carrying it out, it seems all but inevitable.

This historical exploration also shed light on the actors and rationales that shaped the initial capabilities and functions of ICTs. This dissertation started with a meeting between representatives of three of these actors: The State, the military and the RAND Corporation. The latter was the organization for which Paul Baran designed

a communications system that could survive a nuclear attack; a project that would engender the basic method for the routing and transferring of data used over the Internet (Baran, 1960; 1964). Fifty-seven years later, representatives of RAND, the State and the military gathered to discuss how this Cold-War-era technology had been repurposed by their country's then-and-now archenemy. Rand Waltzman's testimony on "the Russian cyber threat" summarized how Russians could leverage the ideation capabilities of ICTs to launch operations aimed to bring about sociopolitical disruption with the use of misinformation. To neutralize this threat, Waltzman prescribed a "whole-of-country" strategy, whereby the State, the private sector, the universities and the Internet data and socialization platforms would join their efforts to push counternarratives—in essence, to neutralize the effect of a cyber-psycho-cognitive operation with another, perhaps preemptive and permanent. This was the first moment when the phenomenon addressed in this dissertation was articulated and acknowledged as an integrated constellation of processes that together could be instrumentalized to execute what Waltzman framed as an act of "information warfare." Paradoxically, by contextualizing it as "a Russian cyber threat," it circumscribed it to the political narrative that was being fed and advanced by the series of Senate Armed Services Committee hearings held in the Winter and the Spring of 2017. Waltzman's testimony served as no less than a discursive instrument in a cyber-psycho-cognitive operation that began during the election of 2016, engendered by Clinton's audacious fusion between the international State-level narrative of Russian hacking and her personal history with State information mishandling.

Clinton's case was particularly elucidating of how malleable and prone to repurposing ICT-driven political narratives can be: in 2013 she fell prey to their destructive power when her long-time confidant's hacked emails revealed she had her own international spy ring, a private email server and, thereafter, a hacker stalker whose persona would haunt her for years to come: Guccifer. Later came the FBI investigations into her email server, the public condemnation for "careless handling of sensitive information" that somehow did not amount to an infringement of the Presidential and Federal Records Act Amendments of 2014 and her portrayal as "the person that gets away with it because of her political position." Given the nature of this controversy, the media's coverage created a discursive context in which her avatar's association with terms such as "email," "email server" and "hacking" became "natural" for the public. As many of these terms had also been used in articles covering recent

incidents of alleged international hacking targeting U.S. institutions, they would eventually provide the media and Clinton herself with the rigging for a future strategic association with the narrative of Russian information warfare.

Some analysts say it began as a result of the American involvement in the fall of Muammar Gaddafi on October 20, 2011; others say it was a reaction to alleged American meddling in the Russian election of 2012; others believed it began as a revenge for the U.S. support of Ukraine's Euromaidan Revolution in February 2014 and the ousting of pro-Russian Ukrainian President, Viktor Yanukovych (Kirk and Wiser, 2017). The hacking of financial, military and government organizations led to the occurrence and mediatization of events in which the use of words and phrases proper of the information warfare discursive framework was common practice, chief among them, articles and news shows covering opinions about cyber threats to national security. Over time, much like it happened to Clinton's avatar, these types of discursive collaborations would create an environment where audiences would accept the mediatized association of "Russians" and "hacks" without requiring as much empirical proof as they might have after the reporting of the first event.

Then, on June 14, 2016, the emergence of the Guccifer 2.0 avatar recontextualized Clinton's own avatar back in the information warfare discursive framework—a remake of her 2013 email scandal (Nakashima, 2016b). However, this time Clinton took control of the narrative by having the Democratic Party keep exclusive access to their computer systems—the alleged crime scene. Government authorities complied with the restrictions imposed by the Democrats and settled for the reports provided by CrowdStrike (Comey, 2017), a company working for the DNC. This is when her portrayal as "a victim of information warfare" and Putin's depiction as "an information warfare aggressor" came together to form a new narrative: Guccifer 2.0 is a body of Russian hackers working directly for Putin himself (Nakashima, 2016b). The media would help to build the bridges between this narrative and yet another which it had begun articulating since late June 2015: the narrative of "Trump's and Putin's mutual admiration" (Bump, 2015c; a; Trump, 2015). However, at the time there was still nothing that could connect Trump to the information warfare discursive framework in which the media was interweaving both the "hacking of the DNC" and "the Russian hacking" narratives.

This changed with Guccifer 2.0's second release, which included emails and documents that confirmed prior suspicions that the Democratic Party had carried out

several kinds of electoral manipulation in order to ensure that Clinton won the party's nomination (Rogers, 2016; Sainato, 2016; Uchill, 2016). Soon after, pressed by reporters for comment on the matter, Trump provided the discursive elements that the media and the Democrats needed to connect his candidate avatar's narrative to "the Russian hacking of the DNC" (Levingston, 2016; Parker and Sanger, 2016a; Roberts *et al.*, 2016; Rucker *et al.*, 2016; Toosi and Kim, 2016). Hereafter the Democrats forced a changed in the media's agenda: instead of focusing on the compromising content of the emails, they should pay attention to "the fact" that not only were the Russians behind the hack of their computer network, but they were also in it to help Trump win the election (Mook, 2016) and the media spent a considerable amount of space and time in its agenda covering and driving this story. Nevertheless, unlike the thousands of emails revealing Clinton's various threads of seemingly unethical and perhaps illicit acts which WikiLeaks would eventually index and make available to the public through a searchable database, the Democrats were never able to produce substantial proof of the alleged collusion between Trump and Putin. Regardless of this, the narrative was designed such that its effects outlived the election.

And they did indeed. Although he holds the title of President of the United States, Donald Trump's legitimacy has been called into question for most of his tenure on the grounds of his alleged treason—a charge that no one was ever able to prove, nor disprove but that threatened to damage his credibility all the same. And, to the extent that the legal system has hampered his ability to wield his power to fulfill campaign promises that garnered him significant support from sectors that were key to his victory, it could also be said that his perceived legitimacy has been curtailed. Again, here I am not referring to the de jure notion of "legitimacy" [22] but rather to the psychological phenomenon that made supporters believed he was "worth" entrusting the power of "the legitimate authority," which in Trump's case was intimately linked to the "reality scenarios" that he constructed with his securitization discourse and the systematic moral and pragmatic disqualification of Clinton. Trump's supporters believed he was going to be able to deliver his "security solutions" for "Protecting the

[22] From a legal standpoint, federal court rulings so far indicate that Trump has tried to execute orders that "exceeded the scope of the authority delegated to him by Congress," and are "antithetical to (…) the founding principles of [the] Nation." It would therefore be hard to argue that the blocking of these actions constituted a curtailment of legitimate authority, for the attempted actions were illegitimate to begin with. However, there is always the possibility that a different judge may have a different opinion on the matter; this certainly appears to be Trump's bet.

Nation from Foreign Terrorist Entry into the United States" (United States, 2017) and they voted for him in exchange. But the beliefs forming the presidentiable avatar for which they voted would be tested through a new chapter in the information warfare narrative of which Clinton had made Trump a part of.

This "postelection chapter" began in the hearings regarding "Russian interference in the 2016 U.S. elections" and "foreign cyber threats to the United States" carried out by the Senate's Select Committee on Intelligence and Armed Services Committee. Time and again, the testimonies given at these extended series of hearings—heard by legislators and everyone with access to C-SPAN—repeatedly mentioned words and phrases that referred to the same objects that the Clinton campaign and the media had spent the last few months associating with Trump (e.g., "Russia," "Putin," "cyber threat," "DNC hacking," etc.). They served, therefore, as instantly mediatized campaigns to erode Trump's legitimacy, who by then had been sworn into office.

Rand Waltzman's testimony before the Senate Armed Services Committee was no exception. It was requested in response to a need to reach clarity on the state of the art of information warfare and the threat that Russia may pose to the U.S. in this regard. This request was only made because of the alleged Russian interference in the 2016 elections. Therefore, the dramatization of such testimony served as an attempt to add "objectivity" to the narrative that was originally devised by the Democrats and which was then being used to weaken Trump's power as president. In this sense, Waltzman's testimony was an instance in which the ongoing cyber-psycho-cognitive operation referenced itself: enunciated as "a Russian threat," the phenomenon was presented to support one of "Russiagate's" discursive pillars, all the while advancing an instantly mediatized narrative designed to undermine the sitting president by providing elements to reinforce the belief that he is a traitor.

At the same time, the enunciation of the phenomenon as a "security issue" before the Senate Armed Services Committee contextualized it above and beyond the particular cyber-psycho-cognitive operation of which the testimony act was part. From an academic viewpoint, it also serves as a pointer to what should come next in the study of the phenomenon. Waltzman's "cognitive security" approach proposed a series of recommendations that seemed to echo the tendencies that Markus Kienscherf observed in his analysis of the domestic and international regimes of American security (Kienscherf, 2013). Like other colonial powers before it, the U.S. has sought to create

conditions of “national security” by influencing international political dynamics to strengthen both its relational and structural power in the system. At the domestic level, this process has led to the implementation of policies oriented to configure a society capable of exercising this international role, including, of course, those policies that have produced the desired results in creating an instrumental order abroad. For example, the War on Terror essentially constructed Arabs as “terrorists;” this led to a dehumanization of people who showed cultural or phenotypical characteristics similar to Middle Easterners’ media portrayal, not just in their home countries, but also in the U.S. This dehumanization was essential to building public support for—among many other despicable acts—their kidnapping and extrajudicial incarceration overseas, and their explicit and implicit curtailment of civil rights granted by the American Constitution. Another example that is more closely related to the topic of this dissertation is the warrantless, allegedly “unintentional” spying of people “located in the U.S.,” making ostensible use of the FISA Amendments Act of 2008 provisions, which established “a procedure for authorizing certain acquisitions of foreign intelligence” via the interception of electronic communications sent or received via any “electronic communication service” by “persons reasonably believed to be located outside of the U.S.” (United States, 2008). In other words, the U.S. legal system authorized the State’s Intelligence Community (IC) to encroach on the private infrastructure of both Internet and web service providers with the express purpose of surveilling people—foreign or not—located outside of the country. Yet the phrasing of such authorization gives the U.S. IC enough latitude to expand the scope of surveillance to include communications from “people located in the U.S.”—so long as it is done “unintentionally.” Once again, ensuring “security” beyond the borders engendered a set of practices whose implementation at home seemed instrumental to the maintenance of the domestic order. Since it was obvious to the authorities that the imposition of a domestic regime of surveillance entered in direct conflict with American civil liberties, they crafted the supporting legal instrument in a way that it did not seemed outright illegitimate.

Short of a new act or set of amendments authorizing the feeding of Waltzman’s “cognitive security” machine with the big data being engineered from these “legally intercepted” communications, this likely instrumentalization may never reach the public light. However, given the abundance of relevant, user-specific data, its great potential as a driver of microtargeted communications and the strategic political alignment

between both the electronic global surveillance and the “cognitive security” initiatives, it almost seems like “a match waiting to happen”—assuming it has not already been consummated. Nevertheless, I believe social scientists should try to find other points of entry into the study of the phenomenon going forward, for this particular path appears to be mined with speculation and the pitfalls it tends to bring along.

In fact, it seems to me that this is precisely what the next step should be: to devise a system of scientific methods to establish the connections between what I put forth as cyber-psycho-cognitive operations’ processual components and the psycho-cognitive changes observable in the trace evidence that may be discovered in online public discourse. Moreover, a secondary, yet indispensable goal that I believe should forever accompany the study of this phenomenon is to design and utilize methods that rigorously segregate what the media publishes as “facts,” from that which should be regarded and presented as “scientific evidence.” It is perfectly understandable for the reader to wonder why such obvious necessity should be raised to the status of “project goal;” after all, what I am recommending amounts to nothing more than applying a basic scientific practice. Yet, believe it or not, the citing of journalistic works as sources of “facts” is not exclusive to journalists. Whether as efforts to advance personal political agendas or not, it appears as even renown scholars are resorting to this.[23]

In a world in which data generated by the public was actually “public” data, choosing the most adequate set of methodologies and methods to study the conditions and critical elements of cyber-psycho-cognitive operations would probably involve crafting a comparison table to facilitate the decision-making process, for all data holding platforms would make their anonymized repositories available to the public and, hence, there would be quite a few options to choose from. However, for an analysis based on actual conditions, elaborating such table is a futile exercise, as it is no coincidence that nearly all scholarship on methodologies and methods for the study

[23] It seems to be that not even the most seasoned of scholars are exempt from the pitfalls of “the era of Post-truth politics.” Kathleen Hall Jamieson’s “Cyberwar: How Russian hackers and trolls helped elect a president” illustrates this point. One would think that a world-renowned scholar who has made a career analyzing both presidents’ discourse and the mediatic discourse on politics, recipient of numerous awards from distinguished research institutions, who is also Director of the University of Pennsylvania’s Annenberg Public Policy Center and co-founder FactCheck.org would be a perfect match for the task of putting to rest the questions lingering after the American presidential election of 2016. Namely, I was expecting to find scientific, sound arguments indicating how indeed Russian meddling in the election of 2016 and Donald Trump’s campaign alleged collusion with Moscow were undeniable “facts.” However, quite regrettably, many assertions requiring such type of evidence cited nothing but articles from commercial news outlets, which are themselves part of one of the cyber-psycho-cognitive operations that I analyzed in this dissertation.

of ICT-mediated psychosocial and sociopolitical phenomena rely on Twitter as their sole source of data. This is what Twitter has been since its early days: the only platform that has provided free API access to its data repository.[24] Not surprisingly, it has also turn it into social scientists' web data source of choice.[25] But even if these practical conveniences did not exist, Twitter's communicational specificities would still make it a uniquely suitable data acquisition instrument for the analysis of cyber psychological operations.

Its uniqueness lies in the capacity to promote material and virtual human-ICT interaction conditions that together precipitate, elicit, propagate and turn datafiable sentimentally-charged expressions whose genuine character is believed to be more likely than that of expressions occurring in other social media platforms. As sentiments reflect the deeper psychological state of the holder, scholars from fields such as computational linguistics have treated users' tweets as information entities which, once enriched with semantic annotations, can be machine-reprocessed for interpretation within the discursive context articulated by all other related "encodings of psychological states." In this regard, Twitter owes its ascribed scientific value to the chain of loose design dependencies that foster a communicational culture where fast and concise actions and reactions take precedence over thoughtfulness, proper grammar and vocabulary.

Sentiment encoding is the product of this asymmetry, for it flourishes best when the communication context calls for spontaneous and unrestrained expression, rather

---

[24] Twitter does this by offering developers three options of preestablished function and procedure sets to place data requests; Twitter's APIs (Application Programming Interface). They differ in the amount, frequency and recency of the data that they can deliver to API users. Developers using Twitter's Search API can send 180 request every 15 minutes and their queries can return an individual user's last 3,200 tweets and up to 5,000 tweets associated to a specific keyword. On the other hand, Twitter's Streaming API does not require queries to return results; it pushes tweets to API users based on preprogrammed criteria in near real-time. However, Twitter limits results to a sample which can vary from 1% to 40% of the total tweets matching the preprogrammed criteria. Finally, there is Twitter's premium Streaming API; Twitter's Firehose: 100% of all tweets matching preprogrammed criteria. Its only inconvenience is that, in contrast to the other two API options, it is costly.

[25] Although of critical importance and consistent throughout the years, Twitter's data access policies are a circumstantial factor, which may change at any time. Facebook recently provided an example of this. Historically, Mark Zuckerberg and company have guarded "their" data according to how they view it —a commodity. If the day came when social scientist could have free data access to socially-produced web data, I would hesitate to select methodologies and methods for the study of cyber psychological operations that are strictly applicable to one platform in particular, for it would be like taking the access to such platform's data as a given, and data access allowances are not necessarily permanent. For the time being, though, we have to work with what we have, which is Twitter-oriented methods and methodologies.

than substantiated arguments, measured statements and strategic thinking. Typical Twitter usage scenarios favor the former over the latter type of cognitive-linguistic experience. And it all begins with Twitter's most basic and distinctive feature: its 280-character message limit.[26] This simple and seamless user interaction design choice preconditions, on the one hand, the material and virtual aspects that define each of Twitter's usage scenarios and, emerging from these, tweets' contextual parameters, that is, the datafiable dimensions of agents' deeper psychological states as expressed through their "tweeted" discourse.

Regarding material representation, a 280-character, message-length limit immediately positions Twitter as a nanocomputing-oriented socialization platform, turning its use on devices with mid- and large-size screens optional and less frequent. Mobile embodiment leads to mobility-oriented discursive construction practices: as tweets' short length allowance lends itself well to fast participation and the platform's discursive functionalities are fully portable, agents perform the act of tweeting as a real-time, collaborative, narrative exercise where contextually-relevant phenomena are co-constructed with the participation of audiences of reactive followers through the sharing of information and views framed as "facts."

Through tweeting, liking, commenting and retweeting, sentiment-permeated ideas and intents of spatiotemporal relevance are indexed in the time and space of their pronouncement and, as they are shared on a community used to providing both real-time and asynchronous feedback, their psycho-cognitive impact becomes equally indexed and traceable through data. Thus, as Twitter impregnates the vastness of discourse in the social web ecosystem through its specific type of dynamism, it also turns it analyzable through the data structures it uses to store users' tweets. Yet, unlike text fields in most common information systems, the tweeting field's 280-character length constraint is matched with a highly robust semantic logic; it may not accept too many characters, but it accepts all kinds.

Furthermore, popular use of this functionality has institutionalized the validity of Twitter-exclusive, ad hoc communicational affordances that amplify and extend characters' semantic capacities on a community-consensus basis. The acceptance of the eventual suspension of rules applicable to formal written language, the resignification of words and the repurposing of signs are but a few examples of

[26] Which in fact used to be 140-characters-long until November 7, 2017.

practices geared towards the maximization of meaning of 280-character sequences. They result in the introduction of increasing semantic heterogeneity into the vastness of social web discourse; various character sequences can convey the same meaning —semantic redundancy— and a single character sequence can have many intended meanings —semantic ambiguity.

The datafication of these types of semantic heterogeneity has given rise to what is both an opportunity and a challenge. “Teaching” neural networks to “learn” and “self-improve their understanding” of the semantic and syntactic nuances permeating the robust output of user-generated content is essential to the mapping of the evolution of web discourse and its impact in the social psyche. The challenge is to “teach” them to “learn on their own” how to accurately discern what character sequences mean in each tweet context, generate meaning from their collective relationship and establish its degree of relevance vis-à-vis specific subjects. Thereafter, the deeper expressions of agents’ psychological states—their sentiments—can be mapped by topic on spacetime and vice versa.

Thus, Twitter accommodates, stimulates and nurtures the types of discursive participation experiences prone to evoking agents’ sentimental expressions. Moreover, it tracks the data points necessary to trace massive psychological state evolution as a function of discursive participation. Therefore, I believe that the most adequate methodologies and methods for the study of cyber-psycho-cognitive operations to date must be Twitter-oriented. At the same time, the fact that Twitter is the only social network to provide open access to its repository also limits the cyber psychological processes that are analyzable.

Nevertheless, whatever the tool and the method, we shall not lose sight of the end goal. Indeed, if “the natural aim of all scientific undertakings is to discover the forces underlying social phenomena and the mode of their operation” (Morgenthau, 1993, p. 18), and international relations is “a science of peace and war” (Aron, 2017, p. 6), then it seems to me that it would only make sense for the field of international relations to begin a concerted, systematic, triple-helix initiative to incorporate scientific methodologies with which cyber-psycho-cognitive operations can be adequately addressed and analyzed above and beyond “the fog of information warfare.” Though the sociocultural, economic and technological conditions of the present may make their total prevention impossible, their “inevitability” may find in science a powerful and formidable opposing force.

REFERENCES

ABRAMSON, H. N. *et al.*, Eds. **Technology Transfer Systems in the United States and Germany: Lessons and Perspectives**. Washington, D.C.: National Academies Pressed, 1997.

ACAR, G. *et al.* The web never forgets: Persistent tracking mechanisms in the wild. *In*: CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 21. 2014, Scottsdale, Arizona. **Conference Paper.** New York, New York: Association for Computing Machinery, 2014. p. 674-689.

ADONI, H.; S. MANE. Media and the social construction of reality: Toward an integration of theory and research. **Communication Research**, Thousand Oaks, California, v. 11, n. 3, p. 323-340, 1984.

AGGARWAL, P. *et al.* **Method and system for providing targeted information based on a user profile in a mobile environment**. Applicant: QUALCOMM INC. Procurer: Pooja Aggarwal, Dilip Krishnaswamy, Robert S. Daley, Patrik Lundqvist. US9497286B2. Filing: June 6, 2008. Publication: November 15, 2016. Google Patents. Available at: https://patents.google.com/patent/US9497286B2. Accessed on: May 19, 2019.

AHMADI, M.; P. DILEEPAN; K. K. WHEATLEY. A SWOT analysis of big data. **Journal of Education for Business**, London, United Kingdom, v. 91, n. 5, p. 289-294, 2016.

AIZCORBE, A.; S. D. OLINER; D. E. SICHEL. Shifting trends in semiconductor prices and the pace of technological progress. **Board of Governors of the Federal Reserve System**, Washington, D.C., September 2006. Available at: https://www.federalreserve.gov/Pubs/FEDS/2006/200644/200644pap.pdf. Accessed on: May 16, 2019.

ALASHRI, S. *et al.* An analysis of sentiments on facebook during the 2016 U.S. presidential election. *In*: Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2016, San Francisco, California. **Conference Paper.** Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 2016. p. 795-802.

ALPEROVITCH, D. **Bears in the midst: Intrusion into the Democratic National Committee**. CrowdStrike. New York, New York: CrowdStrike, 2016. Available at: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

ALTERMAN, E.It's time to stop pretending the Murdochs are in the news business. **The Nation**, New York, New York, n.Issue,2019.

APUZZO, M.; S. LAFRANIERE. 13 Russians indicted as Mueller reveals effort to aid Trump campaign. **The New York Times**, New York, February 16, 2018. Politics. Available at: https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html. Accessed on: April 26, 2019.

ARKIN, W. M.; K. DILANIAN; R. WINDREM. CIA prepping for possible cyber strike against Russia. **NBC News**, New York, October 14, 2016. U.S. News. Available at: https://www.nbcnews.com/news/us-news/cia-prepping-possible-cyber-strike-against-russia-n666636. Accessed on: August 21, 2018.

ARON, R. **Peace & War: A theory of international relations**: with a new introduction by Daniel J. Mahoney & Brian C. Anderson. New York: Routledge, 2017.

ARQUILLA, J.; D. RONFELDT. Cyberwar is Coming! *In*: ARQUILLA, J. e RONFELDT, D. (Ed.). **In Athena's Camp: Preparing for conflict in the Information Age**. Washington, D.C.: RAND Corporation, 1997a. p. 23-60.

_____. A New Epoch—and Spectrum—of Conflict. *In*: ARQUILLA, J. e RONFELDT, D. (Ed.). **In Athena's Camp: Preparing for conflict in the Information Age**. Washington, D.C.: RAND Corporation, 1997b. p. 1-20.

ASSOCIATED PRESS. **Robert Mueller becomes folk hero for Democrats amid Russia investigation**. CBS News. New York, New York: CBS Broadcasting, 2019. Available at: https://www.cbsnews.com/news/robert-mueller-becomes-folk-hero-for-democrats-amid-russia-investigation/. Accessed on: April 15, 2019.

ATKINSON, P. Computer memories: the history of computer form **History and Technology**, Abingdon, United Kingdom, v. 15, n. 1-2, p. 89-120, 1998.

_____. The (in)difference engine: Explaining the disapperance of diversity in the design of the personal computer **Journal of Design History**, Oxford, United Kingdom, v. 13, n. 1, p. 59–72, 2000.

_____. The best laid plans of mice and men: The computer mouse in the history of computing. **Design Issues**, Cambridge, Massachusetts, v. 23, n. 3, p. 46-61, 2007.

BARAN, P. **Reliable digital communications systems using unreliable network repeater nodes**. RAND Corporation. Santa Monica, California: CORPORATION, R., May 27, 1960. Available at: https://www.rand.org/pubs/papers/P1995.html. Accessed on: May 5, 2019.

_____. **On Distributed Communications**. RAND Corporation. Santa Monica, California: RAND CORPORATION, August 1964. Available at: https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf. Accessed on: May 17, 2019.

BARBASH, F. *et al.* Federal courts have ruled against Trump administration policies at least 70 times. **The Washington Post**, Washington, D.C., April 26, 2019. Politics. Available at: https://www.washingtonpost.com/graphics/2019/politics/trump-overruled/?utm_term=.cdb906c9f452. Accessed on: April 29, 2019.

BARBOSA, L.; J. FENG. Robust sentiment detection on Twitter from biased and noisy data. *In*: COLING '10 Proceedings of the 23rd International Conference on Computational Linguistics, 23. 2010, Beijing, China. **Conference Paper.** Stroudsburg, Pennsylvania: Association for Computational Linguistics, 2010. p. 36-44. Available at: http://delivery.acm.org/10.1145/1950000/1944571/p36-barbosa.pdf?ip=189.6.26.118&id=1944571&acc=OPEN&key=4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E6D218144511F3437&__acm__=1558535122_891769cac58416e85e1aac6a01b03d0d.

BARBU, O. Advertising, Microtargeting and Social Media. **Procedia - Social and Behavioral Sciences**, New York, New York, v. 163, p. 44–49, 2014.

BAROCAS, S. The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process. *In*: PLEAD '12 Proceedings of the first edition workshop on Politics, elections and data, 1. 2012, Maui, Hawaii. **Conference Paper.** New York, New York: Association for Computing Machinery, 2012. p. 31-36.

BARR, P. **User-interface metaphors in theory and practice**. 2003. 174 (MSc in Computer Science). Computer Science, Victoria University of Wellington, Wellington, New Zeland.

BARR, P.; R. BIDDLE; J. NOBLE. A taxonomy of user-interface metaphors. *In*: CHINZ '02 Proceedings of the SIGCHI-NZ Symposium on Computer-Human Interaction 3. 2002, Hamilton, New Zeland. **Conference Paper.** Hamilton, New Zeland: Association for Computing Machinery, 2002. p. 25-30.

_____. A semiotic model of user-interface metaphor. *In*: LIU, K. (Ed.). **Virtual, Distributed and Flexible Organisations**. Reading, United Kingdom, 2004. p. 189-215.

BEAN, R. How companies say they're using big data. **Harvard Business Review**, Cambridge, Massachusetts, April 28, 2017. Data. Available at: https://hbr.org/2017/04/how-companies-say-theyre-using-big-data. Accessed on: May 14, 2019.

BECKETT, L. Russian government hackers steal DNC files on Donald Trump. **The Guardian**, San Francisco, June 14, 2016. News: US Politics. Available at: https://www.theguardian.com/technology/2016/jun/14/russian-dnc-hack-donald-trump-files-us-election. Accessed on: April 16, 2019.

BEGEJA, L.; D. C. GIBBON; P. V. VLECK. **Methods and apparatus for dynamic construction of personalized content**. Applicant: AT&T LABS INC. Procurer: Lee Begeja, David C. Gibbon and Paul Van Vleck. US20100058381A1. Filing: September 4, 2008. Publication: March 4, 2010. Google Patents. Available at: https://patents.google.com/patent/US20100058381A1. Accessed on: May 19, 2019.

BERGER, P.; T. LUCKMANN. **The Social Construction of Reality: A Treatise in the Sociology of Knowledge**. New York: Random House, 1966.

BERKOWITZ, D. Work roles and news selection in local TV: Examining the business-journalism dialectic. **Journal of Broadcasting & Electronic Media**, London, United Kingdom, v. 37, n. 1, p. 67–81, 1993.

BERLET, C. Reframing populist resentments in the Tea Party movement. *In*: ROSENTHAL, L. e TROST, C. (Ed.). **Steep : the precipitous rise of the Tea Party**. Berkeley, California: University of California Press, 2012. p. 47-66.

BERNERS-LEE, T. **Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor** New York: HarperSanFrancisco, 1999.

BIDEN, J. **Joe Biden:** Interview [October 2016] Interviewer: TODD, C. New York: NBC, 2016. 40s. Meet The Press' Chuck Todd interviews Vice President Joe Biden on Russian intervention in the U.S. election

BIERMAN, N. 'All of these liars will be sued when the election is over': Donald Trump denounces accusers. **Los Angeles Times**, Los Angeles, California, October 22, 2016. Nation. Available at: https://www.latimes.com/nation/la-na-pol-trump-bravado-20161022-snap-story.html. Accessed on: April 19, 2019.

BINNEY, W. *et al.*Why this is important. **The Nation**, New York, New York, n.Issue,2017.

BLAKE, A. Donald Trump's incredible new defense of his Russia-spying-on-Hillary comments: Just kidding! **The Washington Post**, Washington, D.C., March 2, 2015. The Fix. Available at: https://www.washingtonpost.com/news/the-fix/wp/2016/07/28/donald-trumps-incredible-new-defense-of-his-russia-spying-on-hillary-comments-just-kidding/?utm_term=.7dc304d662e2. Accessed on: April 12, 2019.

_____. Harry Reid's incendiary claim about 'coordination' between Donald Trump and Russia. **The Washington Post**, Washington, D.C., October 31, 2016. The Fix. Available at: https://www.washingtonpost.com/news/the-fix/wp/2016/10/31/harry-reid-just-made-a-huge-incendiary-evidence-free-claim-about-trump-and-russia/?utm_term=.a47b589a2cb7. Accessed on: May 1, 2019.

BOLIN, G.; J. A. SCHWARZ. Heuristics of the algorithm: Big data, user interpretation and institutional translation. **Big Data & Society**, Thousand Oaks, California, v. 2, n. 2, p. 1-12, 2015.

BOND, G. D. *et al.* "Lyin" Ted', "Crooked Hillary", and "Deceptive Donald": Language of lies in the 2016 US presidential debates. **Applied Cognitive Psychology**, v. 31(), n. 6, p. 668-677, 2017.

BOORSTIN, D. J. From news-gathering to news-making: A flood of pseudo-events. *In*: (Ed.). **The Image: A guide to pseudo-events in America**. 25th anniversary ed. New York, New York: Vintage Books, 1992. p. 7-44.

BORGE-HOLTHOEFER, J. *et al.* The dynamics of information-driven coordination phenomena: A transfer entropy analysis. **Science Advances**, Washington, DC, v. 2, n. 4, p. 1-8, 2016.

BORGESIUS, F. Z. *et al.* Online political microtargeting: Promises and threats for democracy. **Utrecht Law Review**, Utrecht, Netherlands, v. 14, n. 1, p. 82-96, 2018.

BOSKER, B. **Life as a tech reporter in the 1970s, At the dawn of the PC age**. The Huffington Post. New York: Oath Inc., 2013. Available at: https://www.huffingtonpost.com/entry/1970s-technology-reporter-victor-mcelheny_n_2695344. Accessed on: August 31, 2018.

BOYD-BARRETT, O. Fake news and "RussiaGate" discourses: Propaganda in the post-truth era. **Journalism**, Thousand Oaks, California, v. 20, n. 1, p. 87–91, 2018.

BOYKOFF, J.; E. LASCHEVER. The Tea Party Movement, framing, and the US Media. **Social Movement Studies**, London, United Kingdom, v. 10, n. 4, p. 341-366, 2011.

BRADNER, E.; D. WRIGHT. Trump says Putin is 'not going to go into Ukraine,' despite Crimea. **CNN**, Atlanta, Georgia, August 1, 2016. Politics. Available at: https://edition.cnn.com/2016/07/31/politics/donald-trump-russia-ukraine-crimea-putin/index.html. Accessed on: April 16, 2019.

BRAUN, J. A.; J. L. EKLUND. Fake News, Real Money: Ad tech platforms, profit-driven hoaxes, and the business of journalism. **Digital Journalism**, London, United Kingdom, v. 7, n. 1, p. 1-21, 2019.

BREAZEAL, J. G. A. C. Manipulating mental states through physical action. *In*: International Conference on Social Robotics 2012, Lecture Notes in Artificial Intelligence 7621, 4. 2012, Chengdu, China. **Conference Paper.** Heidelberg, Germany: Springer-Verlag Berlin Heidelberg, 2012. p. 1-14.

BREWINGTON, A. *et al.* **Russia Indictment 2.0: What to Make of Mueller's Hacking Indictment**. Lawfare. Washington, D.C.: The Lawfare Institute, 2016. Available at: https://www.lawfareblog.com/russia-indictment-20-what-make-muellers-hacking-indictment.

BRIDGE, R. US anti-Russia rhetoric goes nuclear with threats of covert cyber-attacks. **Russia Today**, Moscow, October 21, 2016. Op-ed. Available at: https://www.rt.com/op-ed/362945-american-anti-russia-cyber-attacks/. Accessed on: August 21, 2018.

BRIN, S.; L. PAGE. The anatomy of a large-scale hypertextual web search engine. *In*: Proceedings of the seventh international conference on World Wide Web 7, 7. 1998, Brisbane, Australia. **Conference Paper.** Amsterdam, The Netherlands: Elsevier Science B.V., 1998. p. 107-117. Available at: http://ilpubs.stanford.edu:8090/361/1/1998-8.pdf. Accessed on August 23, 2018.

BUMP, P. Donald Trump isn't fazed by Vladimir Putin's journalist-murdering. **The Washington Post**, Washington, D.C., December 18, 2015. The Fix. Available at: https://www.washingtonpost.com/news/the-fix/wp/2015/12/18/donald-trump-glad-to-be-endorsed-by-russias-top-journalist-murderer/?utm_term=.eea3bf470a7c. Accessed on: May 1, 2019.

_____. Hacked e-mails indicate that Hillary Clinton used a domain registered the day of her Senate hearings. **The Washington Post**, Washington, D.C., March 2, 2015. Available at: https://www.washingtonpost.com/news/the-fix/wp/2015/03/02/hacked-emails-indicate-that-hillary-clinton-used-a-domain-registered-the-day-of-her-senate-hearings/?utm_term=.b9d55b79a89b. Accessed on: April 12, 2019.

_____. Why Donald Trump is praising Vladimir Putin. **The Washington Post**, Washington, D.C., October 1, 2015. The Fix. Available at: https://www.washingtonpost.com/news/the-fix/wp/2015/10/01/why-donald-trump-is-praising-vladimir-putin/?utm_term=.173ef8f78787. Accessed on: May 1, 2019.

_____. No matter how you measure it, Bernie Sanders isn't winning the Democratic primary. **The Washington Post**, Washington, D.C., April 11, 2016. The Fix. Available at: https://www.washingtonpost.com/news/the-fix/wp/2016/04/11/no-matter-how-you-measure-it-bernie-sanders-isnt-winning-the-democratic-primary/?utm_term=.a56ceaccd321. Accessed on: April 11, 2019.

BURKE, K. **A Grammar of Motives** 3rd ed. Berkeley, California: University of California Press, 1969.

BURNYEAT, M. **The Theaetetus of Plato**. Indianapolis, Indiana: Hacket Publishing Company, 1990.

CAMBRIA, E. *et al.* New avenues in opinion mining and sentiment analysis. **IEEE Intelligent Systems**, Institute of Electrical and Electronics Engineers, v. 28, n. 2, p. 15-21, 2013.

CAMPBELL-KELLY, M. Pioneer Profiles - Donald Davies. **Computer Resurrection**, Manchester, United Kingdom, v. 44, n. Autumn 2008, 2008.

CAO, L. *et al.* Behavior Informatics: A New Perspective. **IEEE Intelligent Systems**, Piscataway, New Jersey, v. 29, n. 4, p. 62-80, 2014.

CAPHYON. **Advanced Web Ranking**. Craiova, Romania, April 30, 3019. Available at: https://www.advancedwebranking.com/ctrstudy/. Accessed on: May 22, 2019.

CARR, C. T.; D. Y. WOHN; R. A. HAYES. "Like" as social support: Relational closeness, automaticity, and interpreting social support from paralinguistic digital affordances in social media. **Computers in Human Behavior**, New York, New York, v. 62 p. 385-393, 2016.

CARROLL, J. M.; R. L. MACK; W. A. KELLOGG. Interface metaphors and user interface design. *In*: HELANDER, M. G. (Ed.). **Handbook of human-computer interaction**. 1st ed. Amsterdam: Elsevier Science, 1988. p. 67-85.

CASSIDY, J. Obama's Powerful Message: Donald Trump Is Un-American. **The New Yorker**, New York, July 28, 2016. News & Poltics. Available at: https://www.newyorker.com/news/john-cassidy/obamas-powerful-message-donald-trump-is-un-american. Accessed on: April 15, 2019.

CASTELLS, M. Programming Communication Networks: Media Politics, Scandal Politics, and the Crisis of Democracy. *In*: (Ed.). **Communication Power**. New York: Oxford University Press, 2009. p. 193-298.

_____. **The power of identity**: The information age: economy, society, and culture 2nd ed. Massachusetts: Blackwell Publishers, Inc., 2010a.

_____. **The Rise of the Network Society**: The information age: economy, society, and culture 2nd ed. Massachusetts: Blackwell Publishers, Inc., 2010b.

CERF, V.; R. KAHN. A protocol for packet network intercommunication. **IEEE Transactions on Communications**, Piscataway, New Jersey, v. 22, n. 5, p. 637-648, 1974.

CERUZZI, P. E. **A history of modern computing** 2nd ed. Cambridge, Massachusetts: MIT Press, 2003.

CHADWICK, A. The political information cycle. *In*: (Ed.). **The hybrid media system: Politics and power**. 1st. ed. Oxford, United Kingdom: Oxford University Press, 2013. p. 60-88.

_____. Donald Trump, the 2016 U.S. Presidential Campaign, and the Intensification of the Hybrid Media System. *In*: (Ed.). **The hybrid media system: politics and power**. 2nd ed. New York, New York: Oxford University Press, 2017. p. 240-284.

CHADWICK, A.; J. STROMER-GALLEY. Digital media, power, and democracy in parties and election campaigns: Party decline or party renewal? **The International Journal of Press/Politics**, Thousand Oaks, California, v. 21, n. 3, 2016.

CHANG, A.; P. V. KANNAN. **Customer journey prediction and resolution** Applicant: 24/7 CUSTOMER INC. Procurer: Andrew Chang and Pallipuram V. Kannan. US9092801B2. Filing: August 30, 2012. Publication: July 28, 2015. Google Patents. Available at: https://patents.google.com/patent/US9092801B2. Accessed on: May 19, 2019.

CHEN, A. Why it's time to rethink the laws that keep our health data private. **The Verge**, New York, January 29, 2019. Policy. Available at: https://www.theverge.com/2019/1/29/18197541/health-data-privacy-hipaa-policy-business-science. Accessed on: March 27, 2019.

CHEN, K. *et al.* Building artificial identities in social network using semantic information. *In*: 2011 International Conference on Advances in Social Networks Analysis and Mining 3. 2011, Kaohsiung, Taiwan. **Conference Paper.** Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 2011. p. 565-566. Accessed on May 15, 2019.

CHEYER, A. J.; C. D. BRIGHAM; D. R. GUZZONI. **Determining user intent based on ontologies of domains**. Applicant: APPLE INC. Procurer: Adam John Cheyer, Christopher Dean Brigham and Didier Rene Guzzoni. US8942986B2. Filing: December 21, 2012. Publication: January 27, 2015. Google Patents. Available at: https://patents.google.com/patent/US8942986B2. Accessed on: May 19, 2019.

CHOMSKY, N.; E. S. HERMAN. **Manufacturing Consent: The Political Economy of the Mass Media**. New York: Pantheon Books, 2002.

CHOTINER, I.Is the DNC hack an act of war? **Slate**, New York, n.Issue,2016.

CHOZICK, A. Democrats allege D.N.C. hack is part of Russian effort to elect Donald Trump. **The New York Times**, New York, July 25, 2016. Politics. Available at: https://www.nytimes.com/2016/07/26/us/politics/democrats-allege-dnc-hack-is-part-of-russian-effort-to-elect-donald-trump.html?module=inline. Accessed on: April 6, 2019.

CHUMLEY, C. K. 'Guccifer' hacker sends out Hillary Clinton's memos on Benghazi. **The Washington Times**, Washington, D.C., March 19, 2013. Security. Available at: https://www.washingtontimes.com/news/2013/mar/19/guccifer-hacker-sends-out-hillary-clintons-memos-b/. Accessed on: April 6, 2019.

Computer Networks: The heralds of resource sharing. **Internet Archive**. 26min6s. Available at: https://archive.org/details/ComputerNetworks_TheHeraldsOfResourceSharing. Accessed on September 4, 2018.

CINGEL, D. P.; S. S. SUNDAR. Texting, techspeak, and tweens: The relationship between text messaging and English grammar skills. **New Media & Society**, Thousand Oaks, California, v. 14, n. 8, p. 1304-1320, 2012.

CLAUSEWITZ, C. V. **On War**: Oxford World's Classics. Oxford, United Kingdom: Oxford University Press, 2007.

CLEMENT, S.; D. NAKAMURA. Post-ABC poll: Trump disapproval swells as president, Republicans face lopsided blame for shutdown. **The Washington Post**, Washington, D.C., January 25, 2019. Politics. Available at: https://www.washingtonpost.com/politics/poll-majority-of-americans-hold-trump-and-republicans-responsible-for-shutdown/2019/01/25/e7a2e7b8-20b0-11e9-9145-3f74070bbdb9_story.html?utm_term=.25a72e231f1e. Accessed on: April 28, 2019.

CLINTON, H. R. **What Happened**. New York, New York: Simon & Schuster, 2017.

CODDINGTON, M. The wall becomes a curtain: Revisiting journalism's news-business boundary. *In*: CARLSON, M. e LEWIS, S. C. (Ed.). **Boundaries of journalism: professionalism, practices and participation**. New York, New York: Routledge, 2015. p. 67-82.

CODEVILLA, A. M. Do Economic Sanctions Work? **Strategika**, Washington, D.C., March 29, 2018. Available at: https://www.hoover.org/research/do-economic-sanctions-work. Accessed on: August 22, 2018.

COHEN, M. D. How nuclear proliferation causes conflict: the case for optimistic pessimism. **The Nonproliferation Review**, London, United Kindom, v. 23, n. 3-4, p. 425-442, 2016.

COHN, E. R.; R. W. HADDAD. **Beta Operations: Efficient implementation of a primitive parallel operation**. Department of Computer Science Stanford University. Alexandria, Virginia: AGENCY, D. A. R. P., November 2, 1986.

COLLINSON, S. Who wins if Vladimir Putin meddles in the U.S. election? **CNN**, Atlanta, Georgia, July 26, 2016. Politics. Available at: https://edition.cnn.com/2016/07/26/politics/vladimir-putin-trump-clinton-dnc-hack/. Accessed on: April 15, 2019.

COLLISON, D.; M. LUCOVSKY; C. SJOGREEN. **Assessing advertiser charges for manual user insertion of one or more ads into a document to be made available to another user or users, for distribution of such documents and/or for user actions on such distributed ads**. Applicant: GOOGLE LLC. Procurer: Straub & Pokotylo. US20070198343A1. Filing: May 30, 2006. Publication: August 23, 2007. Google Patents. Available at: https://patents.google.com/patent/US20070198343A1. Accessed on: May 22, 2019.

COMEY, J. B. **Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System**. Washington, D.C.: FBI National Press Office, 2016. Available at: https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system. Accessed on: April 16, 2019.

Open hearing on the Intelligence Community's assessment on Russian activities and intentions in the 2016 U.S. elections: **Hearings before the U.S. Senate Select Committee on Intelligence**, U.S. Senate, 115th Congress.Statement of Hon. James R. Clapper, Director of National Intelligence, Accompanied By: John Brennan, Director of the Central Intelligence Agency; James Comey, Director of the Federal Bureau of Investigation; and Adm. Michael Rogers, Director of the National Security Agency (James B. Comey), p. 5-53, 2017.

CONWAY, L. G.; M. A. REPKE; S. C. HOUCK. Donald Trump as a Cultural Revolt Against Perceived Communication Restriction: Priming Political Correctness Norms Causes More Trump Support. **Journal of Social and Political Psychology**, Trier, Germany, v. 5, n. 1, 2017.

COOK, T. **Keynote address from Tim Cook, CEO, Apple Inc**. Brussels, Belgium: European Data Protection Supervisor, 2018. Available at: https://youtu.be/kVhOLkIs20A. Accessed on: March 25, 2019.

COOLEY, R.; B. MOBASHER; J. SRIVASTAVA. Web Mining: Information and pattern discovery on the World Wide Web. *In*: Proceedings of the Ninth IEEE International Conference on Tools with Artificial Intelligence, 9. 1997. **Conference Paper.** Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 1997. Accessed on May 18, 2019.

CORBATÓ, F. J.; M. M. DAGGETT; R. C. DALEY. An experimental time-sharing system. *In*: AFIPS Conference Proceedings, Volume 21, 1962. **Conference Paper.** Ithaca, New York: AFIPS Press, 1962. p. 335-344. Available at: http://course.sdu.edu.cn/Download/0f22cb53-ad53-44e4-b201-40baffe2bfc3.pdf. Accessed on May 22, 2019.

CORN, D.How the Mueller News Is an Indictment of…Donald Trump and His GOP Enablers. **Mother Jones**, San Francisco, n.Issue,2018.

CORNER, J. Fake news, post-truth and media–political change. **Media, Culture & Society**, Thousand Oaks, California, v. 39, n. 7, p. 1100-1107, 2017.

COULDRY, N.; A. HEPP. **The mediated construction of reality**. Cambridge, United Kingdom: Polity Press, 2017.

_____. The continuing lure of the mediated centre in times of deep mediatization: Media Events and its enduring legacy. **Media, Culture & Society**, Thousand Oaks, California, v. 40, n. 1, p. 114-117, 2018.

CROVITZ, L. G. Donald Trump, Celebrity Politician. **The Wall Street Journal**, New York, March 13, 2016. Available at: https://www.wsj.com/articles/donald-trump-celebrity-politician-1457907805. Accessed on: April 22, 2019.

CROWLEY, M. Was Hillary Clinton running her own rogue intel operation? **The Washington Times**, Washington, D.C., March 18, 2015. Security. Available at: https://www.washingtontimes.com/news/2015/mar/18/monica-crowley-was-hillary-clinton-running-her-own/. Accessed on: April 12, 2019.

CROWLEY, M. **The Democrats' Putin dilemma**. Politico. Arlington, Virginia: John F. Harris, 2016a. Available at: https://www.politico.eu/article/democrats-putin-dilemma-nuclear-news-campaign-diplomacy/. Accessed on: April 18, 2019.

_____. **Trump changed views on Ukraine after hiring Manafort**. Politico. Arlington, Virginia: John F. Harris, 2016b. Available at: https://www.politico.com/story/2016/08/trump-manafort-ukraine-crimea-russia-226573. Accessed on: May 24, 2019.

CROWLEY, M.; T. PAGER. **Trump urges Russia to hack Clinton's email**. Politico. Arlington, Virginia: John F. Harris, 2016. Available at:

https://www.politico.com/story/2016/07/trump-putin-no-relationship-226282. Accessed on: April 15, 2019.

DADDARIO, E. Q. **Incentives and disincentives for proliferation**. Congress of the United States Office of Technology Assessment. Washington, D. C. p. 93-111. Available at: https://www.princeton.edu/~ota/disk3/1977/7705/7705.PDF.

DAVIS, J. H. Hacking of Government Computers Exposed 21.5 Million People. **The New York Times**, New York, July 9, 2015. U.S. Available at: https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html. Accessed on: April 13 2019.

Donna Brazile on passing debate questions onto Hillary camp, democrats funding of Russian research. The View. **YouTube**. November 7, 2017. 5min23s. Available at: https://youtu.be/GLONOYewx8k. Accessed on April 20, 2019.

DEAN, B. **Google's 200 Ranking Factors: The Complete List (2019)**. Backlinko. Unknown: Backlinko LLC, 2018. Available at: https://backlinko.com/google-ranking-factors.

DEBORD, G. **Society of the Spectacle**. London, United Kingdom: Rebel Press, 1992.

DENNARD, R. H. *et al.* Design of ion-implanted MOSFET's with very small physical dimensions. **IEEE Journal of Solid State Circuits**, Piscataway, New Jersey, v. SC-9, n. 5, p. 256–268, 1974.

DENNISTON, L. **New Trump immigration order blocked**. Constitution Daily. Philadelphia, Pennsylvania: National Constitution Center, 2017. Available at: https://constitutioncenter.org/blog/new-trump-immigration-order-blocked. Accessed on: April 30, 2019.

DENTON, R. E., Ed. **The 2016 US Presidential Campaign**. Political Campaigning and Communication. London, United Kingdom: Palgrave Macmillan, Political Campaigning and Communicationed, 2017.

DEPARTMENT OF HOMELAND SECURITY PRESS OFFICE. **Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security**. Washington, D.C.: Department of Homeland Security Press Office, 2016. Available at: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national. Accessed on: April 14, 2019.

DESJARDINS, L. **The giant timeline of everything Russia, Trump and the investigations** PBS NewsHour. New York, New York: Public Broadcasting Service, 2018. Available at: https://www.pbs.org/newshour/features/russia-timeline/.

DEYOUNG, K. FBI: No evidence Clinton's email was hacked by foreign powers, but it could have been. **The Washington Post**, Washington, D.C., July 5, 2016. Politics. Available at: https://www.washingtonpost.com/politics/even-without-charges-fbi-

rebuke-leaves-a-heavy-political-cloud-over-clinton/2016/07/05/79b6f712-42c8-11e6-bc99-7d269f8719b1_story.html?utm_term=.68ee079a99aa. Accessed on: April 16, 2019.

DIAMOND, J.; S. COLLINSON. Democrats accuse Trump of disloyalty over Clinton emails. **CNN**, Atlanta, Georgia, July 28, 2016. Politics. Available at: https://edition.cnn.com/2016/07/27/politics/donald-trump-vladimir-putin-hack-hillary-clinton/index.html. Accessed on: April 15, 2019.

DINAN, S. New emails show possible Benghazi deception by Hillary Clinton, Obama admin. **The Washington Times**, Washington, D.C., June 22, 2015. Politics. Available at: https://www.washingtontimes.com/news/2015/jun/22/new-emails-reignite-hillary-clinton-email-scandal/. Accessed on: April 11, 2019.

DIONNE, E. J. Obama's promise of continuity we can believe in. **The Washington Post**, Washington, D.C. Opinions. Available at: https://www.washingtonpost.com/opinions/obamas-promise-of-continuity-we-can-believe-in/2016/07/27/04778352-5431-11e6-bbf5-957ad17b4385_story.html?utm_term=.5b008a3e3ac1. Accessed on: July 28, 2016

DOCHERTY, C. **Google Ads, a visual history. 2000 – 2018: an 18-year timeline**. Edge45. New York, New York: Edge45 Limited, 2017. Available at: https://edge45.co.uk/blog/google-adwords-evolution-timeline/. Accessed on: May 23, 2019.

DON, A. Narrative and the Interface. *In*: LAUREL, B. e MOUNTFORD, S. J. (Ed.). **The Art of Human-Computer Interface Design**. Boston, Massachusetts: Addison-Wesley Professional, 1990. p. 383-391.

DOVERE, E.-I. **Sanders had big ideas but little impact on Capitol Hill**. Politico. Arlington, Virginia: John F. Harris, 2016. Available at: https://www.politico.com/story/2016/03/bernies-record-220508. Accessed on: April 11, 2019.

Donald Trump: Russia hacking comments were 'sarcastic'. New Day. July 28, 2016. 1min55s. Available at: https://youtu.be/7thZeedJOX8. Accessed on May 14, 2019.

ECKER, W.; W. MÜLLER; R. DÖMER. Hardware-Dependent Software: Introduction and Overview. *In*: (Ed.). **Hardware-Dependent Software**, v.. Dordrecht, The Netherlands: Springer, 2009. p. 1–13.

EDELMAN, R. **Trust and the U.S. presidential election**. Edelman. Chicago. Available at: https://www.edelman.com/trust2017/trust-and-us-presidential-election/.

EHRENFREUND, M. Democratic socialism might be inevitable in America, even if Bernie Sanders loses. **The Washington Post**, Washington, D.C., February 1, 2016. Economic Policy. Available at: https://www.washingtonpost.com/news/wonk/wp/2016/02/01/this-scholar-argues-democratic-socialism-is-not-only-possible-in-america-but-inevitable/?utm_term=.06b50981b0a8. Accessed on: April 11, 2019.

ELECTOME. **The horse race of ideas at the finish line: Tracking the issues Americans did (and didn't) talk about in the 2016 election**. Lab for Social Machines. San Francisco, California: MIT Media Lab, 2016. Available at: https://medium.com/@socialmachines/the-horse-race-of-ideas-at-the-finish-line-1d9dd7a9f178. Accessed on: April 21, 2019.

ELVING, R. **Why are the media obsessed with Trump's controversies and not Clinton's?** NPR. Washington, D.C.: National Public Radio, 2016. Available at: https://www.npr.org/2016/08/11/489576029/why-are-the-media-obsessed-with-trump-s-controversies-and-not-clinton-s. Accessed on: April 21, 2019.

ENGELBART, D. C. **Augmenting Human Intellect: A conceptual framework**. Stanford Research Institute. Menlo Park, California. Available at: http://www.dougengelbart.org/pubs/papers/scanned/Doug_Engelbart-AugmentingHumanIntellect.pdf. Accessed on: September 4, 2018.

The Mother of All Demos. **YouTube**. December 9, 1968. 1hr40min52s. Available at: https://youtu.be/yJDv-zdhzMY. Accessed on September 6, 2018.

_____. **Boosting our Collective IQ** 2nd. ed. Easthampton, Massachusetts: MRW Connected, 2008.

ENLI, G. Twitter as arena for the authentic outsider: exploring the social media campaigns of Trump and Clinton in the 2016 US presidential election. **European Journal of Communication**, Thousand Oaks, California, v. 32, n. 1, p. 50–61, 2017.

ENTEN, H. **Hillary Clinton's Got This**. FiveThirtyEight. New York, New York: The Walt Disney Company, 2016. Available at: https://fivethirtyeight.com/features/hillary-clintons-got-this/. Accessed on: April 11, 2019.

ENTMAN, R. M.; N. USHER. Framing in a fractured democracy: Impacts of digital technology on ideology, power and cascading network activation **Journal of Communication**, Oxford, United Kingdom, v. 68, n. 2, p. 298-308, 2018.

ENTOUS, A.; E. DWOSKIN; C. TIMBERG. Obama tried to give Zuckerberg a wake-up call over fake news on Facebook. **The Washington Post**, Washington, D.C., September 24, 2017. Economy. Available at: https://www.washingtonpost.com/business/economy/obama-tried-to-give-zuckerberg-a-wake-up-call-over-fake-news-on-facebook/2017/09/24/15d19b12-ddac-4ad5-ac6e-ef909e1c1284_story.html?utm_term=.7ee7a190ecf0. Accessed on: April 25, 2019.

EVANS, M. P. Analysing Google rankings through search engine optimization data. **Internet Research**, Bingley, United Kingdom, v. 17, n. 1, p. 21-37, 2007.

EYSENCK, M. W. **Attention and Arousal: Cognition and Performance** 1st. ed. London, United Kingdom: Springer-Verlag Berlin Heidelberg, 1982.

FAIRCLOUGH, N. **Critical Discourse Analysis: The critical study of language**: Language in Social Life. London, United Kingdom: Longman, 1995.

FEDERAL BUREAU OF INVESTIGATION; U.S. DEPARTMENT OF HOMELAND SECURITY. **Grizzly Steppe – Russian Malicious Cyber Activity**. Federal Bureau of Investigation,
U.S. Department of Homeland Security,. Washington, D.C.: (NCCIC), T. N. C. A. C. I. C., December 29, 2016. Available at: https://assets.documentcloud.org/documents/3248231/Report-on-Russian-Hacking.pdf. Accessed on: August 21, 2018.

FELDMAN, J. *et al.* **Preferred cost bidding for online advertising** Applicant: GOOGLE LLC. Procurer: Straub & Pokotylo. US20080255922A1. Filing: April 12, 2007. Publication: October 16, 2008. Google Patents. Available at: https://patents.google.com/patent/US20080255922A1. Accessed on: May 22, 2019.

FERNBACH, P. M. *et al.* Political extremism is supported by an illusion of understanding. **Psychological Science**, Thousand Oaks, California, v. 24, n. 6, p. 939-946, 2013.

FIDLER, D. P. The U.S. election hacks, cybersecurity, and international law. **American Journal of International Law**, Cambridge, United Kingdom, v. 110, p. 337-342, 2016.

FILIPOV, D.; A. ROTH. Moscow had contacts with Trump team during campaign, Russian diplomat says. **The Washington Post**, Washington, D.C., November 10, 2016. Europe. Available at: https://www.washingtonpost.com/world/moscow-had-contacts-with-trump-team-during-campaign-russian-diplomat-says/2016/11/10/28fb82fa-a73d-11e6-9bd6-184ab22d218e_story.html?utm_term=.3bf829452f75. Accessed on: April 12, 2019.

FINANCIAL TIMES EDITORIAL BOARD. America is owed the full contents of the Trump-Russia investigation. **Financial Times**, London, United Kingdom, March 24, 2019. Available at: https://www.ft.com/content/77e9dbaa-4e1b-11e9-b401-8d9ef1626294. Accessed on: April 27, 2019.

FOER, F.Putin’s Puppet. **Slate**, New York, n.Issue,2016.

FOUCAULT, M. Nietzsche, Genealogy, History. *In*: BOUCHARD, D. F. (Ed.). **Language, counter-memory, practice: Selected essays and interviews**. Ithaca, New York: Cornell University Press, 1977. p. 139-164.

_____. **Power/Knowledge: Selected Interviews and Other Writings, 1972-1977** 5th. ed. New York: Pantheon Books, 1980.

_____. **Discipline and Punish: The birth of the prison**. New York: Vintage Books, 1995.

FRANCESCHI-BICCHIERAI, L.Here's the Full Transcript of Our Interview With DNC Hacker 'Guccifer 2.0'. **Motherboard**, New York, n.Issue,2016a.

_____.How hackers broke into John Podesta and Colin Powell's Gmail accounts. **Motherboard**, New York, n.Issue,2016b.

_____.Why does DNC hacker 'Guccifer 2.0' talk like this? **Motherboard**, New York, n.Issue,2016c.

FUCHS, C. Competition and Cooperation in Online Politics. *In*: (Ed.). **Internet and society social theory in the Information Age**. New York: Routledge, 2008a. p. 213-298.

_____. The rise of transnational informational capitalism. *In*: (Ed.). **Internet and society social theory in the Information Age**. New York: Routledge, 2008b. p. 98-120.

_____. Karl Marx and critical media and information studies. *In*: (Ed.). **Foundations of critical media and information studies**. New York: Routledge, 2011. p. 135-160.

GAJARLA, V.; A. GUPTA. **Emotion Detection and Sentiment Analysis of Images**. Georgia: Georgia Institute of Technology, 2015.

GALLO, C. The digital evangelist leading Google's storytelling movement. **Forbes.com**, New York, September 22, 2016. Editor's Pick. Available at: https://www.forbes.com/sites/carminegallo/2016/09/22/the-digital-evangelist-leading-googles-storytelling-movement/#17bdf9f86711. Accessed on: May 14, 2016.

GARTZKE, E. The myth of cyberwar: Bringing war in cyberspace back down to Earth. **International Security**, Cambridge, Massachusetts, v. 38, n. 2, p. 41-73, 2013.

GASS, N. **Former CIA chief: Putin recruited Trump as an 'unwitting agent' of Russia**. Politico. Arlington, Virginia: John F. Harris, 2016. Available at: https://www.politico.com/story/2016/08/michael-morell-endorses-clinton-226707. Accessed on: April 23, 2019.

GATTI, M. A. D. C. *et al.* Handling big data on agent-based modeling of Online Social Networks with MapReduce. *In*: Proceedings of the Winter Simulation Conference 2014, 2014, Savannah, Georgia. **Conference Paper.** Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 2014. p. 851-862.

GERTH, J.; S. BIDDLE. **Leaked Private Emails Reveal Ex-Clinton Aide's Secret Spy Network**. Gawker. New York: Bustle Digital Group, 2015. Available at: https://gawker.com/leaked-private-emails-reveal-ex-clinton-aides-secret-sp-1694112647.

GHITIS, F. Trump encourages Putin, America's foe. **CNN**, Atlanta, Georgia, July 28, 2016. Politics. Available at: https://edition.cnn.com/2016/07/27/opinions/trump-putin-email-hack-ghitis/index.html. Accessed on: April 15, 2019.

GIDDENS, A. **The Constitution of Society: Outline of the Theory of Structuration**. Oxford: Polity Press, 1984.

GIFFIN, K. The contribution of studies of source credibility to a theory of interpersonal trust in the communication process. **Psychological Bulletin**, Washington, D.C., v. 68, n. 2, p. 104-120, 1967.

GILLANI, N. *et al.* Me, My Echo Chamber, and I: Introspection on Social Media Polarization. *In*: Proceedings of the 2018 World Wide Web Conference 27. 2018, Lyon, France. **Conference Paper.** New York, New York: Association for Computing Machinery, 2018. p. 823-831.

GOFFMAN, E. **The presentation of self in everyday life**. Edinburgh, Scotland: University of Edinburgh Social Sciences Research Centre, 1956.

GOLDSMITH, J. **What is old, and new, and scary in Russia's probable DNC hack**. Lawfare. Washington, D.C.: The Lawfare Institute, 2016. Available at: https://www.lawfareblog.com/what-old-and-new-and-scary-russias-probable-dnc-hack.

GOMER, R. *et al.* Network analysis of third-party tracking: User exposure to tracking cookies through search. *In*: WI-IAT '13 Proceedings of the 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence, 12. 2013, Atlanta, Georgia. **Conference Paper.** Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 2013. p. 549-556.

Chomsky: By Focusing on Russia, Democrats Handed Trump a “Huge Gift” & Possibly the 2020 Election. Democracy Now! **YouTube**. April 18, 2019. 10min47s. Available at: https://youtu.be/sLyS0E91H1o. Accessed on May 17, 2019.

GOOGLE. **About similar audiences for Search**. Mountain View, California. Available at: https://support.google.com/google-ads/answer/7151628. Accessed on: May 20, 2019.

_____. **About similar audiences on the Display Network**. Mountain View, California. Available at: https://support.google.com/google-ads/answer/2676774. Accessed on: May 20, 2019.

_____. **Cost-per-click (CPC): Definition**. Mountain View, California. Available at: https://support.google.com/google-ads/answer/116495. Accessed on: May 20, 2019.

_____. **Google Academy for Ads**. Mountain View, California. Available at: https://landing.google.com/academyforads/faq.html. Accessed on: May 20, 2019.

_____. **Smart Goals**. Mountain View, California. Available at: https://support.google.com/analytics/answer/6153083. Accessed on: May 20, 2019.

GOOGLE TRENDS. **Searches for Hillary Clinton on election week**. Google Trends. Mountain View, California: Google.com, 2016. Available at: https://trends.google.com/trends/story/US_cu_jRvIwFYBAAATWM_en_en-US. Accessed on: April 22, 2019.

GOTTFRIED, J.; E. SHEARER. **News use across social media platforms 2016**. Pew Research Center. Washington, D.C., May 26, 2016. Available at: https://www.journalism.org/wp-content/uploads/sites/8/2016/05/PJ_2016.05.26_social-media-and-news_FINAL-1.pdf. Accessed on: April 19, 2019.

GRAHAM, D. A. An intelligence report that will change no one's mind. **The Atlantic**, New York, January 6, 2017. Politics. Available at: https://www.theatlantic.com/politics/archive/2017/01/odni-report-on-russian-hacking/512465/. Accessed on: April 26, 2019.

GRANBERG-RADEMACKER, J. S.; K. PARSNEAU. Tweet you very much: An analysis of candidate Twitter usage from the 2016 Iowa Caucus to Super Tuesday. *In*: (Ed.). **The Role of Twitter in the 2016 US Election**. New York: Palgrave Macmillan, 2018. p. 21-44.

GREENBERG, A.Hack Brief: Russia's Breach of the DNC Is About More Than Trump's Dirt. **Wired**, New York, n.Issue,2016.

GREENWALD, G. A Consensus Emerges: Russia Committed an "Act of War" on Par With Pearl Harbor and 9/11. Should the U.S. Response Be Similar? **The Intercept**, New York, February 19, 2018. Glenn Greenwald. Available at: https://theintercept.com/2018/02/19/a-consensus-emerges-russia-committed-an-act-of-war-on-par-with-pearl-harbor-and-911-should-the-u-s-response-be-similar/. Accessed on: August 21, 2018.

GREENWALD, G.; L. FANG. EXCLUSIVE: New Email Leak Reveals Clinton Campaign's Cozy Press Relationship. **The Intercept**, New York, October 9, 2016. Glenn Greenwald. Available at: https://theintercept.com/2016/10/09/exclusive-new-email-leak-reveals-clinton-campaigns-cozy-press-relationship/. Accessed on: April 20, 2019.

GROSHEK, J.; K. KOC-MICHALSKA. Helping populism win? Social media use, filter bubbles, and support for populist presidential candidates in the 2016 US election campaign. **Information, Communication & Society**, London, United Kingdom, v. 20, n. 9, p. 1389-1407, 2017.

GROSS, D.How Bernie Sanders, the Socialist, Quietly Entered the Top 4% of Earners. **Fortune**, New York, n.Issue,2016.

GRUDIN, J. The computer reaches out: the historical continuity of interface design. *In*: CHI '90 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 8. 1990, Seattle, Washington. **Conference Paper.** New York, New York: Association for Computing Machinery, 1990. p. 262-268. Accessed on May 15, 2019.

_____. A moving Target — The Evolution of Human-Computer Interaction. *In*: JACKO, J. A. (Ed.). **Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications**. 3rd ed. Boca Raton, Florida: CRC Press, 2012. p. xxvii-lix.

GRUNDY, A. F.; J. GRUNDY. **Women and Computers**. Exeter, United Kingdom: Intellect Books, 1996.

GUCCIFER 2.0. **Guccifer 2.0 DNC's servers hacked by a lone hacker**. Guccifer 2.0. San Francisco, California: Guccifer 2.0, 2016. Available at: https://guccifer2.wordpress.com/2016/06/15/dnc/. Accessed on: April 12, 2019.

GUHA, R. **Generating and presenting advertisements based on context data for programmable search engines**. Applicant: GOOGLE LLC. Procurer: Ramanathan Guha. US20070038614A1. Filing: August 10, 2005. Publication: February 15, 2007. Google Patents. Available at: https://patents.google.com/patent/US20070038614A1. Accessed on: May 22, 2019.

_____. **Search result ranking based on trust**. Applicant: GOOGLE LLC. Procurer: Ramanathan Guha. US7603350B1. Filing: May 9, 2006. Publication: Octubre 13, 2009. Google Patents. Available at: https://patents.google.com/patent/US7603350B1. Accessed on: May 22, 2019.

GUHA, R. V. *et al.* **Query identification and association**. Applicant: GOOGLE LLC. Procurer: Ramanathan V. Guha, Shivakumar Venkataraman, Vineet Gupta, Gokay Baris Gultekin, Pradnya Karbhari and Abhinav Jalan. US8631003B2. Filing: April 30, 2012. Publication: January 14, 2014. Google Patents. Available at: https://patents.google.com/patent/US8631003B2. Accessed on: May 22, 2019.

GUHA, S. *et al.* TweetGrep: Weakly Supervised Joint Retrieval and Sentiment Analysis of Topical Tweets. *In*: Tenth International AAAI Conference on Web and Social Media, 10. 2016, Cologne, Germany. **Conference Paper.** Menlo Park, California: Association for the Advancement of ArtificialIntelligence, 2016. p. 161-170. Available at: https://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13030. Accessed on August 2, 2018.

GUNTHER, A. C. The Persuasive Press Inference: Effects of mass media on perceived public opinion **Communication Research**, Thousand Oaks, California, v. 25, n. 5, p. 486-504.

GUO, L.; C. VARGO. "Fake News" and emerging online media ecosystem: An integrated intermedia agenda-setting analysis of the 2016 U.S. presidential election. **Communication Research**, Thousand Oaks, California, p. 1-23, 2018.

HABERMAS, J. **The Theory of Communicative Action: Lifeworld and System: A Critique of Functionalist Reason**. Massachusetts: Beacon Press, 1987.

_____. **Legitimation Crisis**. Oxford, UK: Polity Press, 1992.

HAEG, A. **The funnel & the news business**. Medium. San Francisco, California: A Medium Corporation, 2018. Available at: https://medium.com/groundsource-notes/the-funnel-the-news-business-596bfd29db8d. Accessed on: April 21, 2019.

HAIGH, M. Stopping Fake News: The work practices of peer-to-peer counter propaganda. **Journalism Studies**, London, United Kingdom, v. 19, n. 14, 2018.

HALPIN, H. **Social Semantics: The search for meaning on the web**: Semantic Web and Beyond: Computing for Human Experience. New York: Springer, 2013.

HAM, J. *et al.* The automaticity of social behavior towards robots: The influence of cognitive load on interpersonal distance to approachable versus less approachable robots. *In*: International Conference on Social Robotics 2012, Lecture Notes in Artificial Intelligence 7621, 4. 2012, Chengdu, China. **Conference Paper.** Heidelberg, Germany: Springer-Verlag Berlin Heidelberg, 2012. p. 15-25.

HAMMOND, K. J. The value of big data isn't the data. **Harvard Business Review**, Cambridge, Massachusetts, May 1, 2013. Technology. Available at: https://hbr.org/2013/05/the-value-of-big-data-isnt-the. Accessed on: May 14, 2019.

HARRIS, S. Hillary's secret email was a cyberspy's dream weapon. **The Daily Beast**, New York, New York, March 7, 2015. Cheat Sheet. Available at: https://www.thedailybeast.com/hillarys-secret-email-was-a-cyberspys-dream-weapon. Accessed on: April 12, 2019.

_____. Obama to Putin: Stop Hacking Me. **The Daily Beast**, New York, New York, April 8, 2015. Cheat Sheet. Available at: https://www.thedailybeast.com/obama-to-putin-stop-hacking-me. Accessed on: April 26, 2019.

HARVEY, D. **The Condition of Postmodernity**. Oxford: Wiley-Blackwell, 1991.

_____. The Fetish of Technology: Causes and Consequences. **Macalester International**, Saint Paul, Minnesota, v. 13, n. 7, 2003.

HAWAII (DISTRICT). United States District Court for the District of Hawaii. **Order granting motion for temporary restraining order**. 440 Other Civil Rights. Violation of 5th & 8th Amendments. 28 U.S.C. § 1331. Plaintiffs: State of Hawaii, Ismail Elshikh, John Does 1 & 2, and Muslim Association of Hawaii, Inc. Defendants: Donald J. Trump, Elaine Duke and Rex Tillerson. Judge: DERRICK K. WATSON. Submitted: Honolulu, Hawaii, October 17, 2017. U.S. Government Publishing Office: Honolulu, Hawaii, CV. NO. 17-00050 DKW-KSC, October 17, 2017. Available at: https://www.govinfo.gov/content/pkg/USCOURTS-hid-1_17-cv-00050/pdf/USCOURTS-hid-1_17-cv-00050-6.pdf. Accessed on: May 17, 2019.

HAWKINS, J. A. **Doctrine for Joint Psychological Operations**. Washington, D.C.: Chairman of the Joint Chiefs of Staff, 2003.

HAYDEN, M. V. Former CIA chief: Trump is Russia's useful fool. **The Washington Post**, Washington, D.C., November 3, 2016. Opinions. Available at: https://www.washingtonpost.com/opinions/former-cia-chief-trump-is-russias-useful-fool/2016/11/03/cda42ffe-a1d5-11e6-8d63-3e0a660f1f04_story.html?utm_term=.150cffcff97d. Accessed on: April 11, 2019.

HAYDEN, M. V. *et al.* **Statenent by former national-security officials**. Washington, D.C.: A.G. Sulzberger, 2016. Available at: https://www.nytimes.com/interactive/2016/08/08/us/politics/national-security-letter-trump.html?module=inline. Accessed on: April 19, 2019.

HEALEY, C. **Sentiment Viz: Tweet Sentiment Visualization** North Carolina. Available at: https://www.csc2.ncsu.edu/faculty/healey/tweet_viz/tweet_app/. Accessed on: November 8.

HEART, F. *et al.* The interface message processor for the ARPA computer network. *In*: Proceedings of the 1970 Spring Joint Computer Conference, 1970, Atlantic City, New Jersey. **Conference Paper.** New York, New York: Association for Computing Machinery, 1970. p. 551-567. Available at: http://www.walden-family.com/public/1970-imp-afips.pdf.

HEIM, J. Nancy Pelosi on impeaching Trump: 'He's just not worth it'. **The Washington Post**, Washington, D.C., March 11, 2019. The Washington Post Magazine. Available at: https://www.washingtonpost.com/news/magazine/wp/2019/03/11/feature/nancy-pelosi-on-impeaching-president-trump-hes-just-not-worth-it/?utm_term=.618b4922cdcb. Accessed on: April 27, 2019.

HELSPER, E. J. A Corresponding Fields Model for the Links Between Social and Digital Exclusion. **Communication Theory**, Oxford, United Kingdom, v. 22, n. 4, p. 403-426, 2012.

HENDRICKS, J. A.; D. SCHILL. The Social Media Election of 2016. *In*: DENTON, R. E. (Ed.). **The 2016 US Presidential Campaign**. London, United Kingdom: Palgrave Macmillan, 2017. p. 121-150.

HENRIKSEN, A. The end of the road for the UN GGE process: The future regulation of cyberspace. **Journal of Cybersecurity**, Oxford, United Kingdom, v. 5, n. 1, p. 1-9, 2019.

HEUVEL, K. V.Editor's note regarding Patrick Lawrence's article "A new report raises big questions about last year's DNC hack". **The Nation**, New York, New York, n.Issue,2017.

HIRSCHHEIM, R. A. The effect of a priori views on the social implications of computing: The case of office automation **ACM Computing Surveys**, New York, New York, v. 18, n. 2, p. 165-195, 1986.

HODAS, N. O.; K. LERMAN. How visibility and divided attention constrain social contagion. *In*: Proceedings of the 2012 ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust, 1-9. 2012, Amsterdam, Netherlands. **Conference Paper.** Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 2012. Accessed on May 21, 2019.

HOLLAND, S.; E. STEPHENSON. Trump draws ire after urging Russia to find 'missing' Clinton emails. **Reuters**, London, July 27, 2016. Politics. Available at: https://www.reuters.com/article/us-usa-election-trump-cyber-idUSKCN10723A. Accessed on: April 15, 2019.

HOLTON, R. Deciding to trust, coming to believe. **Australasian Journal of Philosophy**, London, United Kingdom, v. 72, n. 1, p. 63-76, 1994.

HUBINETTE, C. F. **Determining proximity to topics of advertisements** Applicant: GOOGLE LLC. Procurer: Carl F. Hubinette. US8549032B1. Filing: February 5, 2013. Publication: October 1, 2013. Google Patents. Available at: https://patents.google.com/patent/US8549032B1. Accessed on: May 22, 2019.

HWANG, T.; L. ROSEN. Harder, better, faster, stronger: International law and the future of online PSYOPS. **ComProp Working Paper No. 1**, Oxford, United Kingdom, January 17, 2017. Research. Available at: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/02/Comprop-Working-Paper-Hwang-and-Rosen.pdf.

IOFFE, J.Why This Russian Wants to Give Donald Trump 100,000 Rubles. **Politico**, Arlington, Virginia, n.Issue,2016.

JACOBS, B. WikiLeaks cables: Tunisia blocks site reporting 'hatred' of first lady. **The Guardian**, Washington, D.C., June 16, 2016. US Politics. Available at: https://www.theguardian.com/us-news/2016/jun/15/six-things-we-learned-dnc-hacked-donald-trump. Accessed on: April 16, 2019.

JAMIESON, K. H. **Cyberwar: How Russian hackers and trolls helped elect a president**. New York: Oxford University Press, 2018.

JOHNSON, A. **'Allegedly' Disappears as Russians Blamed for DNC Hack**. Fair.org. New York, New York: Fairness & Accuracy In Reporting, Inc., 2016. Available at: https://fair.org/home/allegedly-disappears-as-russians-blamed-for-dnc-hack/.

JONES, K. Trust as an affective attitude. **Ethics**, Chicago, Illinois, v. 107, n. 1, p. 4-25, 1996.

JORDAN, B. US still has no definition for cyber act of war. **Military.com**, New York, New York, June 22, 2016. News. Available at: https://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html. Accessed on: April 5, 2019.

JOSEPH S. NYE, J. New Approaches to Nuclear Proliferation Policy. **Science**, Washington, D.C., v. 256, n. 5061, p. 1293-1297, 1992.

KAHNEMAN, D. **Attention and Effort** 1st. ed. Englewood Cliffs, New Jersey: Prentice-Hall, 1973.

KANG, C.; S. FRENKEL. Facebook says Cambridge Analytica harvested data of up to 87 million users. **The New York Times**, New York, April 4, 2018. Technology.

Available at: https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html. Accessed on: February 5, 2019.

President Trump claims 'complete and total exoneration' after Mueller report. ABC World News Tonight. **YouTube**. March 24, 2019. 3min53s. Available at: https://youtu.be/YFxGtObzIY0. Accessed on April 27, 2019.

KARAZY, S.; M. WILLIAMS. Senator McCain says Russia must pay price for hacking. **Reuters**, Washington D.C., December 30, 2016. World News. Available at: https://www.reuters.com/article/us-usa-russia-cyber-mccain-idUSKBN14J1LW. Accessed on: April 28, 2018.

KATZ, N. *et al.* **User controlled multi-device media-on-demand system**. Applicant: ROVI TECHNOLOGIES CORP. Procurer: Neil Katz, Bruce P. Semple, Edith H. Stern, Barry E. Willner. US9307291B2. Filing: July 13, 2011. Publication: April 5, 2016. Google Patents. Available at: https://patents.google.com/patent/US9307291B2. Accessed on: May 19, 2019.

KAUSHIK, A. **See, Think, Do, Care Winning Combo: Content +Marketing +Measurement!** Occam's Razor. Denver, Colorado: Avinash Kaushik, 2015. Available at: https://www.kaushik.net/avinash/see-think-do-care-win-content-marketing-measurement/. Accessed on: May 14, 2019.

KAUSHIK, L.; A. SANGWAN; J. H. L. HANSEN. Sentiment extraction from natural audio streams. *In*: Proceedings of 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, 38. 2013, Vancouver, Canada. **Conference Paper.** Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 2013.

KEARNEY, M. W. Analyzing change in network polarization. **New Media & Society**, Thousand Oaks, California, p. 1-23, 2019.

KELLY, C. **Former Obama mentor: Trump's Russian hack 'jokes' could 'constitute treason'**. Politico. Arlington, Virginia: John F. Harris, 2016. Available at: https://www.politico.com/story/2016/07/laurence-tribe-trump-russia-226371. Accessed on: April 5, 2019.

KENNEDY, C. *et al.* An evaluation of the 2016 election polls in the United States. **Public Opinion Quarterly**, Oxford, United Kingdom, v. 82, n. 1, p. 1-33, 2017.

KEREN, A. Trust and belief: a preemptive reasons account. **Synthese**, New York, New York, v. 191, n. 12, p. 2593-2615, 2014.

KHARPAL, A. **Russian hackers target NATO, military secrets**. CNBC. New Jersey: NBC, 2014. Available at: https://www.cnbc.com/2014/10/28/russian-hackers-target-nato-military-secrets.html. Accessed on: April 13, 2019.

KIENSCHERF, M. **US Domestic and International Regimes of Security: Pacifying the globe, securing the homeland**. New York: Routledge, 2013.

KILDALL, G. A.Introducing the new and improved IBM PC. $49[95]. **PC Mag**, New York, v. 4, n.Issue,1985.

KIOUSIS, S. *et al.* Competing for Attention: Information Subsidy Influence in Agenda Building during Election Campaigns. **Journalism & Mass Communication Quarterly**, Thousand Oaks, California, v. 86, n. 3, p. 545–562, 2009.

KIOUSIS, S.; J. STRÖMBÄCK. The White House and public relations: Examining the linkages between presidential communications and public opinion. **Public Relations Review**, New York, New York, v. 36, n. 1 p. 7–14, 2010.

Putin's Revenge. Frontline. **Public Broadcasting Service**. October 25, 2017. 3hr8min Available at: https://www.pbs.org/wgbh/frontline/film/putins-revenge/.

KISSINGER, H. **World Order: Reflections on the character of nations and the course of history**. New York, New York: Penguin Books, 2014.

KLEINBERG, J. M. Authoritative sources in a hyperlinked environment. **Journal of the ACM**, New York, New York, v. 46, n. 5, p. 604-632, 1999.

KLEINROCK, L. Time-shared systems: A theoretical treatment. **Journal of the ACM**, New York, New York, v. 14, n. 2, p. 242-261, 1967.

KOPAN, T. DNC hack: What you need to know. **CNN**, Atlanta, Georgia, June 21, 2016. Politics. Available at: https://edition.cnn.com/2016/06/21/politics/dnc-hack-russians-guccifer-claims/index.html. Accessed on: April 16, 2019.

KUBE, C.; J. MIKLASZEWSKI. **Russia hacks Pentagon computers: NBC, citing sources**. NBC News. New Jersey: NBC, 2015. Available at: https://www.cnbc.com/2015/08/06/russia-hacks-pentagon-computers-nbc-citing-sources.html. Accessed on: August 6, 2015.

KUHN, T. S. **The structure of scientific revolutions** 3. Chicago: The University of Chicago Press, 1996.

KUHN, W.; A. U. FRANK. A formalization of metaphors and image-schemas in user interfaces. *In*: MARK, D. M. e FRANK, A. U. (Ed.). **Cognitive and Linguistic Aspects of Geographic Space**. Dordrecht, Netherlands: Springer, 1991. p. 419-434.

LAWRENCE, P.A new report raises big questions about last year's DNC hack. **The Nation**, New York, New York, n.Issue,2017.

LAWRENCE, S.; C. L. GILES.Searching the World Wide Web. **Science**, Washington, D.C., v. 280, n.Issue, p. 98-100,1998.

_____. Accessibility of information on the web. **Nature**, London, United Kingdom, v. 400, n. 6740, p. 107-107, 1999.

LAZER, D. M. J. *et al.* The science of fake news. **Science**, Washington, D.C., v. 359, n. 6380, p. 1094-1096, 2018.

LEAN, T.A brave new world: the 1980s home computer boom. **BBC History Magazine**, London, n.Issue,2016.

LEHOVEC, K. Invention of p-n junction isolation in integrated circuits. **IEEE Transactions on Electron Devices**, Piscataway, New Jersey, v. 25, n. 4, p. 495-496, 1978.

LEMAY, A. *et al.* Survey of publicly available reports on advanced persistent threat actors. **Computers & Security**, New York, New York, v. 72, p. 26-59, 2018.

LEOPOLD, J. He Solved The DNC Hack. Now He's Telling His Story For The First Time. **BuzzFeed News**, New York, November 8, 2017. Trending. Available at: https://www.buzzfeednews.com/article/jasonleopold/he-solved-the-dnc-hack-now-hes-telling-his-story-for-the. Accessed on: April 13, 2019.

LEVINGSTON, I. **Trump: I hope Russia finds 'the 30,000 emails that are missing**. CNBC. New Jersey: NBC, 2016. Available at: https://www.cnbc.com/2016/07/27/trump-hope-russia-finds-the-30000-emails-that-are-missing.html. Accessed on: April 15 2019.

LEWIS, R. C. *et al.* **Platform for mobile advertising and microtargeting of promotions**. Applicant: QUALCOMM INC Procurer: Robert C. Lewis, Giridhar D. Mandyam, Anthony M. Sheehan, Martin C. Dickens. US20090197582A1. Filing: January 28, 2009. Publication: August 6, 2009. Google Patents. Available at: https://patents.google.com/patent/US20090197582A1/en. Accessed on: April 20, 2019.

LIBERTY, J. **The Electome: Where political journalism meets AI**. MIT Media Lab. Cambridge, Massachusetts: Massachusetts Institute of Technology, 2017. Available at: https://www.media.mit.edu/videos/sm-electome-2017-01-31/. Accessed on: May 22, 2019.

LICKLIDER, J. C. R. Man-Computer Symbiosis. **IRE Transactions on Human Factors in Electronics**, Palo Alto, California, v. HFE-1, n. 1, p. 4–11, 1960.

_____. **Memorandum For Members and Affiliates of the Intergalactic Computer Network**. Washington, D.C., 1963. Available at: http://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network. Accessed on: September 6, 2018.

On-line man-computer communication. Proceedings of the May 1-3, 1962, spring joint computer conference, Number., Year, San Francisco, California. **Type of Work.** San Francisco, California, Year. Accessed on: September 4, 2018.

LIPPMANN, W. **Public Opinion**. New York: Free Press, 1997.

LIPTAK, K. Obama says it's 'possible' Putin is trying to sway vote for Trump. **CNN**, Atlanta, Georgia, July 27, 2016. Politics. Available at: https://edition.cnn.com/2016/07/26/politics/obama-possible-putin-trying-to-sway-vote-for-trump/index.html. Accessed on: April 15, 2019.

LIU, B. **Sentiment Analysis and Opinion Mining**: Synthesis Lectures on Human Language Technologies. California: Morgan & Claypool Publishers, 2012.

_____. **Sentiment Analysis: Mining opinions, sentiments, and emotions**: Synthesis Lectures on Human Language Technologies. New York: Cambridge University Press, 2015.

LLOYD, M.; L. A. FRIEDLAND. Introduction: Solving America's communication crisis. *In*: LLOYD, M. e FRIEDLAND, L. A. (Ed.). **The communication crisis in America, and how to fix it**. New York, New York: Palgrave Macmillan, 2016. p. xxvii-xxx.

LORD, C. The Psychological Dimension in National Strategy. *In*: LORD, C. e BARNETT, F. R. (Ed.). **Political warfare and pyschological operations: Rethinking the US approach**. New York, New York: National Defense University Press, 1989.

MAHONEY, M. S. The History of Computing in the History of Technology. **IEEE Annals of the History of Computing**, Piscataway, New Jersey, v. 10, n. 2, p. 113–125, 1988.

MAI, J.-E. Big data privacy: The datafication of personal information. **The Information Society**, London, United Kingdom, v. 32, n. 3, p. 192-199, 2016.

MANIMALA, M. J. Sustainable development through ICT: The need for entrepreneurial action. *In*: MANIMALA, M. J.;MITRA, J.*, et al* (Ed.). **Enterprise support systems: An international perspective**. New Delhi: SAGE Publications India, 2009. p. 121-138.

MANOLARAKIS, C. *et al.* **Cross-Channel User Tracking Systems, Methods and Devices** Applicant: VELTI MOBILE PLATFORMS LIMITED. Procurer: Christos Manolarakis, Mark Sutterlin, Andrew Milkowski, Guowei Zhang, Stephanie Luxenberg, Rick Landsman and Maurice J. Carron. US20140120864A1. Filing: March 15, 2013. Publication: May 1, 2014. Google Patents. Available at: https://patents.google.com/patent/US20140120864A1. Accessed on: April 20, 2019.

MARLAND, A. Political photography, journalism, and framing in the digital age: The management of visual media by the Prime Minister of Canada. **The International Journal of Press/Politics**, Thousand Oaks, California, v. 17, n. 2, p. 214–233, 2012.

MARR, B. **Big data in practice: How 45 successful companies used big data analytics to deliver extraordinary results**. West Sussex, United Kingdom: Wiley, 2016.

MARTIN, A. Digital literacy and the "digital society". *In*: LANKSHEAR, C. e KNOBEL, M. (Ed.). **Digital Literacies: Concepts, Policies and Practices**. 1st. ed. New York, New York: Peter Lang, 2008. p. 151-176.

MARTIN, C.; S. HOPE; S. ZUBAIRI. **The role of digital exclusion in social exclusion**. Ipsos MORI. Edinburgh, Scotland: TRUST, T. C. U., September 2016. p. 1-45.

MARX, K. **The Eighteenth Brumaire of Louis Napoleon**. Moscow, Russia: Dodo Press, 2009.

MATSA, K. E.; K. LU. 10 facts about the changing digital news landscape. **FactTank**, Washington, D.C., September 14, 2016. FactTank. Available at: https://www.pewresearch.org/fact-tank/2016/09/14/facts-about-the-changing-digital-news-landscape/. Accessed on: May 22, 2019.

MAYER, J. R.; J. C. MITCHELL. Third-Party Web Tracking: Policy and Technology. *In*: Proceedings of the 2012 IEEE Symposium on Security and Privacy, 33. 2012, San Francisco, California. **Conference Paper.** Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 2012. Accessed on May 22, 2019.

MAZZA, E. Donald Trump Tells Bill O'Reilly It's 'An Eye For An Eye' In War With Fox News. **HuffPost**, New York, January 28, 2016. Media. Available at: https://www.huffpostbrasil.com/entry/donald-trump-fox-news-eye-for-an-eye_n_56a9790fe4b0016489225a54. Accessed on: April 19, 2019.

MAZZEIA, M. J.; D. NOBLE. Big data dreams: A framework for corporate strategy. **Business Horizons**, New York, New York, v. 60, n. 3, p. 405-414, 2017.

MAZZETTI, M.; K. BENNER. Mueller finds no Trump-Russia conspiracy, but stops short of exonerating president on obstruction. **The New York Times**, New York, March 24, 2019. Politics. Available at: https://www.nytimes.com/2019/03/24/us/politics/mueller-report-summary.html. Accessed on: April 27, 2019.

MCCAIN, J. **John McCain:** Interview [December 2016] Interviewer: UNKNOWN. Kiev, Ukraine: 1+1 Media Group, 2016. 2min. Ukrainian 1+1 channel interviews senator John McCain on Russian interference in the U.S. election.

Hearing to receive testimony on foreign cyber threats to the United States: **Hearings before the Senate Armed Services Committee**, U.S. Senate, 115th Congress.Opening Statement on Foreign Cyber Threats (John McCain), p. 2-7, 2017.

MCCOMBS, M. The Future Agenda for Agenda Setting Research. **Journal of Mass Communication Studies**, Tokyo, Japan, v. 45, 1994.

_____. **Setting the Agenda: The Mass media and public opinion** 2nd. Cambridge, United Kingdom: Polity, 2014.

MCHALE, J. P. Media coverage of corruption and scandal in the 2016 presidential election: Fantasy themes of Crooked Hillary and Corrupt Businessman Trump. *In*: (Ed.). **Corruption, Accountability and Discretion**. Bingley, United Kingdom: Emerald Group Publishing, 2017. p. 107-123.

MCLAUGHLIN, S.; S. A. MILLER. Clinton emails reveal Blumenthal influential in crafting diplomacy. **The Washington Times**, Washington, D.C., July 1, 2015 Security. Available at: https://www.washingtontimes.com/news/2015/jul/1/hillary-clinton-emails-did-include-classified-info/. Accessed on: April 11, 2019.

MITCHELL, A. **Andrea Mitchell:** Interview [June 2016] Interviewer: WILLIAMS, B. New York, New York: MSNBC, 2016. 3min19s. NBC News' chief foreign affairs correspondent provides a rationale for Guccifer 2.0's theft of the Clinton campaign's dossier on Donald Trump. .

MONINO, J.-L. Data Value, Big Data Analytics, and Decision-Making. **Journal of the Knowledge Economy**, New York, New York, v. 7, n. 1, p. 1-12, 2016.

MOOK, R. **Robby Mook:** Interview [July 2016] Interviewer: TAPPER, J. Atlanta, Georgia: Turner Broadcasting System, Inc., 2016. 2min8s. Hillary Clinton's campaign manager accusses Donald Trump of collusion with Russian State actors. .

MOORE, G. E. Cramming more components onto integrated circuits. **Electronics**, New York, New York, v. 38, n. 8, p. 114-117, 1965.

MORELL, M. J. I Ran the C.I.A. Now I'm Endorsing Hillary Clinton. **The New York Times**, New York, August 5, 2016. Opinion. Available at: https://www.nytimes.com/2016/08/05/opinion/campaign-stops/i-ran-the-cia-now-im-endorsing-hillary-clinton.html. Accessed on: May 14, 2019.

MORGENTHAU, H. **Politics among nations : The struggle for power and peace** 6th. Beijing: Peking University Press, 1993.

MOWERY, D. C.; R. LANGLOIS. The federal government role in the development of the U.S. software industry. *In*: MOWERY, D. C. (Ed.). **The international computer software industry: A comparative study of industrial evolution and struture**. New York: Oxford University Press, 1996. p. 53-85.

MURRAY, G. R.; A. SCIME. Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies. **Journal of Political Marketing**, London, United Kingdom, v. 9, n. 3, p. 143–166, 2010.

NAJJAR, M. S.; W. J. KETTINGER. Data Monetization: Lessons from a retailer's journey. **MIS Quarterly Executive**, Atlanta, Georgia, v. 12, n. 4, p. 213-225, 2013.

NAKASHIMA, E. Cyber-intruder sparks response, debate. **The Washington Post**, Washington, D.C., December 8, 2011. National Security. Available at: https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html?utm_term=.8dceeb860b43. Accessed on: April 14, 2019.

_____. Hackers breach some White House computers. **The Washington Post**, Washington, D.C., October 28, 2014. National Security. Available at: https://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html?utm_term=.fe3d3535fddf. Accessed on: April 14, 2019.

_____. Russian hackers use 'zero-day' to hack NATO, Ukraine in cyber-spy campaign. **The Washington Post**, Washington, D.C., October 13, 2014. National Security. Available at: https://www.washingtonpost.com/world/national-security/russian-hackers-use-zero-day-to-hack-nato-ukraine-in-cyber-spy-campaign/2014/10/13/f2452976-52f9-11e4-892e-602188e70e9c_story.html?utm_term=.afd90d45b9a0. Accessed on: April 13, 2019.

_____. Cyber researchers confirm Russian government hack of Democratic National Committee. **The Washington Post**, Washington, D.C., June 20, 2016. National Security. Available at: https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html?utm_term=.29e8ff8d2852. Accessed on: April 16, 2019.

_____. 'Guccifer 2.0' claims credit for DNC hack. **The Washington Post**, Washington, D.C., June 15, 2016. National Security. Available at: https://www.washingtonpost.com/world/national-security/guccifer-20-claims-credit-for-dnc-hack/2016/06/15/abdcdf48-3366-11e6-8ff7-7b6c1998b7a0_story.html?utm_term=.80867d274ffc. Accessed on: April 12, 2019.

_____. National intelligence director: Hackers have targeted 2016 presidential campaigns. **The Washington Post**, Washington, D.C., May 18, 2016. National Security. Available at: https://www.washingtonpost.com/world/national-security/national-intelligence-director-hackers-have-tried-to-spy-on-2016-presidential-campaigns/2016/05/18/2b1745c0-1d0d-11e6-b6e0-c53b7ef63b45_story.html?utm_term=.0a592746db2f. Accessed on: April 14, 2019.

_____. New details emerge about 2014 Russian hack of the State Department: It was 'hand to hand combat'. **The Washington Post**, Washington, D.C., April 3, 2017. National Security. Available at: https://www.washingtonpost.com/world/national-security/new-details-emerge-about-2014-russian-hack-of-the-state-department-it-was-hand-to-hand-combat/2017/04/03/d89168e0-124c-11e7-833c-503e1f6394c9_story.html?utm_term=.62c7eb2d1741. Accessed on: April 6, 2019.

_____. Russian government hackers penetrated DNC, stole opposition research on Trump. **The Washington Post**, Washington, D.C., June 14, 2016. National Security. Available at: https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?utm_term=.0bae10f46a23. Accessed on: April 14, 2019.

NAMBIAR, R.; M. POESS. Transaction Performance vs. Moore's Law: A Trend Analysis. *In*: NAMBIAR, R. e POESS, M. (Ed.). **Performance Evaluation,**

Measurement and Characterization of Complex Systems, v.6417. Berlin, Germany: Springer, 2011.

NEALE, D. C.; J. M. CARROLL. The role of metaphors in user interface design. *In*: HELANDER, M. G.;LANDAUER, T. K.*, et al* (Ed.). **Handbook of Human Computer Interaction**. 2nd ed. Amsterdam: Elsevier Science, 1997. p. 441-458.

NESBIT, J. Donald Trump's many, many, many, many ties to Russia. **TIME**, New York, August 15, 2016. Politics. Available at: http://time.com/4433880/donald-trump-ties-to-russia/.

NORTON, B. **DNC emails: Wasserman Schultz furiously pressured MSNBC after it criticized her "unfair" treatment of Sanders**. Salon. San Francisco, California: Salon Media Group, 2016. Available at: https://www.salon.com/2016/07/22/dnc_emails_wasserman_schultz_furiously_pressured_msnbc_after_it_criticized_her_unfair_treatment_of_sanders/. Accessed on: April 20, 2019.

NOYCE, R. Microelectronics. **Scientific American**, New York, New York, v. 23, n. 3, p. 63-69, 1977.

OBAMA, B. **Barack Obama:** Interview [July 2016] Interviewer: GUTHRIE, S. New York: NBC News, 2016a. 1min44s. Savannah Guthrie inteviews President Barack Obama on Russian involvement in the DNC hack.

President Obama: Russia hacked the DNC. Bloomberg Politics. **YouTube**. December 16, 2016. 4min14s. Available at: https://youtu.be/y3Y_S_KJT8E. Accessed on August 21, 2018.

Watch President Barack Obama's full speech at the 2016 Democratic National Convention. **YouTube**. July 27, 2016. 49min9s. Available at: https://youtu.be/aip0BAWrdLw. Accessed on April 18, 2019.

OBEIDALLAH, D. Why Trump will never be presidential. **CNN**, Atlanta, Georgia, July 26, 2016. Politics. Available at: https://edition.cnn.com/2016/07/25/opinions/trump-cant-be-presidential-obeidallah/index.html. Accessed on: April 15, 2019.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. **Intelligence Community Assessment: Assessing Russian activites and intentions in recent US elections**. National Intelligence Council. Washington, D.C.: COUNCIL, N. I., January 6, 2017. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf. Accessed on: April 26, 2019.

OHLIN, J. D. Did Russian cyber-interference in the 2016 election violate international law? **Social Science Research Network**, New York, New York, 2017.

OPRYSKO, C. **Schiff says impeachment still possible even if Russia probe clears Trump**. Politico. Arlington, Virginia: John F. Harris, 2019. Available at: https://www.politico.com/story/2019/03/13/schiff-trump-impeachment-russia-probe-1219471. Accessed on: April 27, 2019.

ORESKES, N.; E. M. CONWAY. Challenging Knowledge: How climate science became a victim of the Cold War. *In*: PROCTOR, R. N. e SCHIEBINGER, L. L. (Ed.). **Agnotology : the making and unmaking of ignorance**. Stanford, California: Stanford University Press, 2008. p. 37-54.

OSBORN, A. Putin ally tells Americans: vote Trump or face nuclear war. **Reuters**, London, October 12, 2016. Politics. Available at: https://www.reuters.com/article/us-usa-election-russian-trump/putin-ally-tells-americans-vote-trump-or-face-nuclear-war-idUSKCN12C28Q. Accessed on: November 11, 2017.

OUELLETTE, L. The Trump Show. **Television & New Media**, Thousand Oaks, California, v. 17, n. 7, p. 647-650, 2016.

PAGE, L. *et al.* The PageRank citation ranking: Bringing order to the web. **Stanford InfoLab**, Stanford, California, January 29, 1998. Available at: http://ilpubs.stanford.edu:8090/422/1/1999-66.pdf. Accessed on: May 22, 2019.

PAN, B. *et al.* In Google We Trust: Users' Decisions on Rank, Position, and Relevance. **Journal of Computer-Mediated Communication**, Oxford, United Kingdom, v. 12, n. 3, p. 801-823, 2007.

PANETTA, L. Ex-CIA director: Trump 'not qualified' to be President. **CNN**, Atlanta, July 27, 2016. Amanpour. Available at: https://edition.cnn.com/videos/world/2016/07/27/intv-amanpour-leon-panetta-trump-presidential-election.cnn. Accessed on: April 18, 2019.

PARKER, A.; D. E. SANGER. Donald Trump Calls on Russia to Find Hillary Clinton's Missing Emails. **The New York Times**, New York, July 27, 2016. Politics. Available at: https://www.nytimes.com/2016/07/28/us/politics/donald-trump-russia-clinton-emails.html. Accessed on: April 15, 2019.

_____. Donald Trump's Appeal to Russia Shocks Foreign Policy Experts. **The New York Times**, New York, July 28, 2016. Europe. Available at: https://www.nytimes.com/2016/07/29/world/europe/russia-trump-clinton-email-hacking.html. Accessed on: April 15, 2019.

PARMELEE, J. H. The agenda-building function of political tweets. **New Media & Society**, Thousand Oaks, California, v. 16, n. 3, p. 434–450, 2013.

PATTERSON, T. E. **News coverage of the 2016 general election: How the press failed the voters**. Harvard Kennedy School. Harvard, Massachusetts: HARVARD KENNEDY SCHOOL SHORENSTEIN CENTER ON MEDIA, P. A. P. P. p. 22. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2884837. Accessed on: April 11, 2019.

_____. **News coverage of the 2016 national conventions negative news, lacking context**. Harvard Kennedy School. Harvard, Massachusetts: HARVARD KENNEDY SCHOOL SHORENSTEIN CENTER ON MEDIA, P. A. P. P. p. 22.

Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2884835. Accessed on: April 11, 2019.

_____. **News coverage of the 2016 presidential primaries Horse-race reporting has consequences**. Harvard Kennedy School. Harvard, Massachusetts: HARVARD KENNEDY SCHOOL SHORENSTEIN CENTER ON MEDIA, P. A. P. P. p. 22. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2884834. Accessed on: April 11, 2019.

PELKEY, J. Networking: Vision and Packet Switching 1959 - 1968: Intergalactic Vision to Arpanet. *In*: PELKEY, J. (Ed.). **Entrepreneurial Capitalism & Innovation: A history of computer communications 1968 -1988** Brea, California: New Dream Network, LLC, 2007.

PEREZ, E.; S. PROKUPECZ. How the U.S. thinks Russians hacked the White House. **CNN**, Atlanta, Georgia, April 8, 2015. Politics. Available at: https://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html. Accessed on: August 21, 2018.

_____. Sources: State Dept. hack the 'worst ever'. **CNN**, Atlanta, Georgia, March 10, 2015. Politics. Available at: https://edition.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/index.html. Accessed on: August 21, 2018.

PERLER, C. **System and method for collection, aggregation, analysis, reporting, and monetization of personal data generated across heterogeneous systems and devices**. Filing: September 24, 2009. Publication: August 15, 2013https://patents.google.com/patent/US20090240568A1/en. Accessed on: April 20, 2019.

_____. **System and method for collection, aggregation, analysis, reporting, and monetization of personal data generated across heterogeneous systems and devices**. Procurer: Craig Perler. US20130211876A1. Filing: August 15, 2013. Publication: December 19, 2012. Google Patents. Available at: https://patents.google.com/patent/US20130211876A1. Accessed on: May 17, 2019.

PERLROTH, N.; D. GELLES. Russian Hackers Amass Over a Billion Internet Passwords. **The New York Times**, New York, August 5, 2014. Technology. Available at: https://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?hp&action=click&pgtype=Homepage&version=LedeSum&module=first-column-region&region=top-news&WT.nav=top-news. Accessed on: April 13, 2019.

PHILLIPS, A. Mueller's indictment of 12 Russians lands at a really awkward moment for Trump. **The Washington Post**, Washington, D.C., July 13, 2018. The Fix. Available at: https://www.washingtonpost.com/news/the-fix/wp/2018/07/13/muellers-indictment-of-12-russians-lands-at-a-really-awkward-moment-for-trump/?utm_term=.188c6b9a2e53. Accessed on: April 26, 2019.

PINCHUK, D. DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach **The Guardian**, New York, July 26, 2016. US Politics. Available at: https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2. Accessed on: April 16, 2019.

_____. Putin dismisses US threat of retaliation over alleged hacking. **The Guardian**, New York, October 16, 2016. US Politics. Available at: https://www.theguardian.com/world/2016/oct/16/putin-russia-us-democrats-hacking-cyber-attacks. Accessed on: August 21, 2018.

PODKALICKA, A.; E. MILNE; J. KENNEDY. Introduction. *In*: (Ed.). **Grand Designs: Consumer markets and home-making**. . London, United Kingdom: Palgrave Macmillan, 2018. p. 1-30.

POLETTI, A.; J. RAK. Introduction: Digital Dialogues. *In*: POLETTI, A. e RAK, J. (Ed.). **Identity Technologies: Constructing the Self online**. 1st. ed. Madison, Wisconsin: The University of Wisconsin Press, 2014. p. 3-24.

PORIA, S. *et al.* Context-dependent sentiment analysis in user-generated videos. *In*: Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), 55. 2017, Vancouver, Canada. **Conference Paper.** Stroudsburg Pennsylvania: Association for Computational Linguistic, 2017. p. 873-883.

POUZIN, L. Presentation and major design aspects of the CYCLADES computer network. *In*: Proceedings of the Third ACM Symposium on Data Communications and Data Networks Analysis and Design, 3. 1973, New York, New York. **Conference Paper.** New York, New York: Association for Computing Machinery, 1973. p. 80-87. Accessed on May 22, 2019.

PROCTOR, R. W.; K.-P. L. VU. Human information processing: An overview for human-computer interaction. *In*: JACKO, J. A. (Ed.). **Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications**. 3rd ed. Boca Raton, Florida: CRC Press, 2012. p. 21-40.

RAINSFORD, S. US election 2016: Why Russia is celebrating Trump win. **BBC News**, Moscow, Russia, November 9, 2016. US Election 2016. Available at: https://www.bbc.com/news/election-us-2016-37928171. Accessed on: August 15, 2016.

RAMER, J.; A. SOROCA; D. DOUGHTY. **Aggregation and enrichment of behavioral profile data using a monetization platform**. Applicant: JUMPTAP INC. Procurer: Jorey Ramer, Adam Soroca and Dennis Doughty. US20090240568A1. Filing: March 9, 2009. Publication: September 24, 2009. Google Patents. Available at: https://patents.google.com/patent/US20090240568A1/en. Accessed on: April 20, 2019.

_____. **Aggregation of behavioral profile data using a monetization platform** Applicant: JUMPTAP INC. Procurer: Jorey Ramer, Adam Soroca and Dennis Doughty. US20090240568A1. Filing: March 9, 2009. Publication: September 17,

2009. Google Patents. Available at: https://patents.google.com/patent/US20090234711A1. Accessed on: April 20, 2019.

RANGANATHAN, S. R. **Colon Classification** 6th. ed. New Delhi, India: Ess Ess Publications, 2006.

Rebuilding America Now New TV Ad: Hillary Clinton: More of the Same. **YouTube**. June 5, 2016. 30s. Available at: https://youtu.be/9t54Ly_mvuk.

REGAN, M. D. **Hillary Clinton wins the Nevada Democratic caucuses**. New York, New York, February 20, 2016. Available at: https://www.pbs.org/newshour/politics/clinton-sanders-in-close-race-in-nevada-caucuses. Accessed on: April 11.

REIMER, J. A history of the GUI. **ARS Technica**, New York, New York, May 5, 2005. Available at: https://arstechnica.com/features/2005/05/gui/4/. Accessed on: May 22, 2019.

REISINGER, D.How Russian Hackers Spiked the Currency Exchange Rate. **Fortune**, New York, n.Issue,2016.

RICE, R. E.; H. GILES. The contexts and dynamics of science communication and language. **Journal of Language and Social Psychology**, Thousand Oaks, California, v. 36, n. 1, p. 127-139, 2017.

RID, T. **Cyber war will not take place**. Oxford, United Kingdom: Oxford University Press, 2013.

RILEY, M.How Russian Hackers Stole the Nasdaq. **Bloomberg Businessweek**, New York, n.Issue,2014.

RITCHIE, H. **Read all about it: The biggest fake news stories of 2016**. CNBC. New Jersey: NBC, 2016. Available at: https://www.cnbc.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html. Accessed on: May 2, 2019.

RITZER, G. Automating prosumption: The decline of the prosumer and the rise of the prosuming machines. **Journal of Consumer Culture**, Thousand Oaks, California, v. 15, n. 3, p. 407-424, 2015.

RITZER, G.; N. JURGENSON. Production, Consumption, Prosumption: The nature of capitalism in the age of the digital ‘prosumer’. **Journal of Consumer Culture**, Thousand Oaks, California, v. 10, n. 1, p. 13-36, 2010.

ROBERTS, D. *et al.* Donald Trump to Russia: hack and publish Hillary Clinton's 'missing' emails. **The Guardian**, New York, July 27, 2016. US Politics. Available at: https://www.theguardian.com/us-news/2016/jul/27/donald-trump-russia-hillary-clinton-emails-dnc-hack. Accessed on: April 15, 2019.

ROBERTS, L. G. The evolution of packet switching. **Proceedings of the IEEE**, Piscataway, New Jersey, v. 66, n. 11, p. 1307-1313, 1978.

ROGERS, E. M.; J. W. DEARING. Agenda-Setting Research: Where has it been, where is it going? **Annals of the International Communication Association**, London, United Kingdom, v. 11, n. 1, p. 555-594, 1988.

ROGERS, J. **After DNC attack, hacker Guccifer 2.0 claims Hillary Clinton 'dossier' leak**. Fox News. New York, New York: Fox, 2016. Available at: https://www.foxnews.com/tech/after-dnc-attack-hacker-guccifer-2-0-claims-hillary-clinton-dossier-leak.

ROSE, F.The Power of Immersive Media. **Strategy + Business**, New York, New York, n.Issue,2015.

ROSEN, S. Electronic Computers: A historical survey. **ACM Computing Surveys**, New York, New York, v. 1, n. 1, p. 7-36, 1969.

ROSENTHAL, S. *et al.* Sentiment Analysis in Twitter. *In*: Proceedings of the 8th International Workshop on Semantic Evaluation (SemEval 2014), 8. 2014, Dublin, Ireland. **Conference Paper.** Stroudsburg, Pennsylvania: Association for Computational Linguistics, 2014. p. 73–80. Available at: http://www.aclweb.org/anthology/S14-2009.

ROSENZWEIG, P.Mueller's Blockbuster Indictment. **The Atlantic**, Boston, n.Issue,2018.

ROTH, A.; D. FILIPOV. Kremlin spokesman vows retaliation against U.S. sanctions. **The Washington Post**, Washington, D.C., December 29, 2016. World. Available at: https://www.washingtonpost.com/world/kremlin-spokesman-vows-retaliation-against-us-sanctions/2016/12/29/e0126be2-ce08-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.8d7fd10eee8e. Accessed on: May 16, 2019.

RUCKER, P.; R. COSTA; J. A. DELREAL. Trump invites Russia to meddle in the U.S. presidential race with Clinton's emails. **The Washington Post**, Washington, D.C., July 27, 2016. Politics. Available at: https://www.washingtonpost.com/politics/trump-invites-russia-to-meddle-in-the-us-presidential-race-with-clintons-emails/2016/07/27/a85d799e-5414-11e6-b7de-dfe509430c39_story.html?utm_term=.7b1863be2f97. Accessed on: April 15, 2019.

RUMSFELD, D. H. **Information Operations Roadmap**. Washington, D.C.: The U.S. Department of Defense, 2003.

SADOWSKI, J. When data is capital: Datafication, accumulation, and extraction. **Big Data & Society**, Thousand Oaks, California, v. 6, n. 1, p. 1-12, 2019.

SAINATO, M. **Guccifer 2.0 Leak Reveals How DNC Rigged Primaries for Clinton**. Observer. New York, New Yrok: Joseph Meyer, 2016. Available at: https://observer.com/2016/06/guccifer-2-0-leak-reveals-how-dnc-rigged-primaries-for-clinton/.

SALEM, H.; S. WALKER; L. HARDING. Crimean parliament seized by unknown pro-Russian gunmen. **The Guardian**, Simferopol
Kiev, February 27, 2014. World: Europe. Available at: https://www.theguardian.com/world/2014/feb/27/crimean-parliament-seized-by-unknown-pro-russian-gunmen. Accessed on: April 25, 2019.

SALVANTO, A. *et al.* **Pelosi has edge over Trump on budget negotiations, CBS News poll shows**. CBS News. New York, New York: CBS Broadcasting, 2019. Available at: https://www.cbsnews.com/news/pelosi-has-edge-over-trump-on-budget-negotiations-says-cbs-news-poll/. Accessed on: April 28, 2019.

SANGER, D. E.; N. CORASANITI. D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump. **The New York Times**, New York, June 14, 2016. Politics. Available at: https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html. Accessed on: April 15, 2019.

SANGER, D. E.; C. SAVAGE. U.S. says Russia directed hacks to influence elections. **The New York Times**, New York, October 7, 2016. Politics. Available at: https://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html. Accessed on: April 24, 2019.

SAVAGE, C.; N. PERLROTH. Is D.N.C. Email Hacker a Person or a Russian Front? Experts Aren't Sure. **The New York Times**, New York, July 27, 2016. Politics. Available at: https://www.nytimes.com/2016/07/28/us/politics/is-dnc-email-hacker-a-person-or-a-russian-front-experts-arent-sure.html. Accessed on: April 16, 2019.

SCHATZ, B. A history of Donald Trump's bromance with Vladimir Putin. **Mother Jones**, San Francisco, October 5, 2016. Politics. Available at: https://www.motherjones.com/politics/2016/10/trump-putin-timeline/.

SCHIPPER, B. C.; H. WOO. Political awareness, microtargeting of voters, and negative electoral campaigning. **Social Science Research Network**, New York, New York, 2017.

SCHLEIFER, T.; D. WALSH. McCain: Russian cyberintrusions an 'act of war'. **CNN**, Atlanta, Georgia, December 31, 2016. Politics. Available at: https://edition.cnn.com/2016/12/30/politics/mccain-cyber-hearing/index.html. Accessed on: April 27, 2019.

SCHMIDT, M. S. Hillary Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules. **The New York Times**, New York, March 2, 2015. Politics. Available at: https://www.nytimes.com/2015/03/03/us/politics/hillary-clintons-use-of-private-email-at-state-department-raises-flags.html?_r=0. Accessed on: April 11, 2019.

SCHMIDT, M. S.; M. APUZZO. Hillary Clinton Emails Said to Contain Classified Data. **The New York Times**, New York, July 24, 2015. Politics. Available at: https://www.nytimes.com/2015/07/25/us/politics/hillary-clinton-email-classified-

information-inspector-general-intelligence-community.html. Accessed on: April 11, 2019.

SCHULBERG, J. Intelligence report concludes that Vladimir Putin intervened in U.S. election to help Donald Trump win. **HuffPost**, New York, January 6, 2017. Politics. Available at: https://www.huffpostbrasil.com/entry/intelligence-report-russia-hack-election_n_586fed0fe4b02b5f8588b94a. Accessed on: April 26, 2019.

SCHULTHEIS, E. **FBI Director Comey: Agency requested access to DNC servers**. CBS News. New York, New York: CBS Broadcasting, 2017. Available at: https://www.cbsnews.com/news/fbi-director-comey-agency-requested-access-to-dnc-servers/. Accessed on: April 15, 2019.

SCIUTTO, J.; N. GAOUETTE; K. LIPTAK. 'Little doubt' Russia behind DNC hack, US official says. **CNN**, Atlanta, Georgia, July 27, 2016. Politics. Available at: https://edition.cnn.com/2016/07/27/politics/dnc-hacking-emails-russia-white-house/index.html. Accessed on: April 15, 2019.

SEIDEL, R. J.; R. E. ANDERSON; B. HUNTER. **Computer Literacy: Issues and Directions for 1985**. Cambridge, Massachusetts: Academic Press, 1982.

SHARMA, J. **Using search query information to determine relevant ads for a landing page of an ad**. Applicant: GOOGLE LLC. Procurer: Straub & Pokotylo. US7603350B1. Filing: December 30, 2005. Publication: July 5, 2007. Google Patents. Available at: https://patents.google.com/patent/US20070156520. Accessed on: May 22, 2019.

SHMUELI, G. Analyzing behavioral big data: Methodological, practical, ethical, and moral issues. **Quality Engineering**, London, United Kingdom, v. 29, n. 1, p. 57-74, 2017.

SHURKIN, J. N. **Engines of the mind: The evolution of the computer from mainframes to microprocessors**. New York: Norton, 1996.

SIDES, J.; M. TESLER; L. VAVRECK. The 2016 U.S. Election: How Trump lost and won. **Journal of Democracy**, Baltimore, Maryland, v. 28, n. 2, p. 34-44, 2017.

SIMMONS, W. L.; S. N. CATANZARO. **Creation and usage of synthetic user identifiers within an advertisement placement facility** Applicant: DATAXU INC. Procurer: Willard L. Simmons and Sandro N. Catanzaro. US20120323674A1. Filing: June 29, 2012. Publication: December 20, 2012. Google Patents. Available at: https://patents.google.com/patent/US20120323674A1. Accessed on: May 19, 2019.

SIMONYAN, M. Kremlin: Russia faces unprecedented cyber-threats from the US. **Russia Today**, Moscow, October 15, 2016. World News. Available at: https://www.rt.com/news/362868-kremlin-cyberattack-threats-us/. Accessed on: August 21, 2018.

_____. Putin on Biden cyberthreat: First time US admits such thing on highest level **Russia Today**, Moscow, October 16, 2016. World News. Available at:

https://www.rt.com/news/362936-putin-brics-press-conference/. Accessed on: August 21, 2018.

SLOBODIAN, N.; I. PTASNYK. Sanctions on Russia: Effectiveness and Impacts. **Europe Now**, New York, New York, April 24, 2019. February 5, 2018. Available at: https://www.europenowjournal.org/2019/02/04/sanctions-on-russia-effectiveness-and-impacts/.

SLOMAN, S.; P. FERNBACH. **The knowledge illusion: Why we never think alone** 1st. edition. New York: River Books, 2017.

SMALE, A.; M. D. SHEAR. Russia Is Ousted From Group of 8 by U.S. and Allies. **The New York Times**, New York, March 24, 2014. Europe. Available at: https://www.nytimes.com/2014/03/25/world/europe/obama-russia-crimea.html. Accessed on: April 12, 2019.

SMITH, A. Donald Trump blasts 'liars' in the media for coverage of his Saddam Hussein praise. **Business Insider**, New York, New York, July 7, 2016. Available at: https://www.businessinsider.com/donald-trump-blasts-media-saddam-hussein-2016-7. Accessed on: April 19, 2019.

SNYDER, M. T. Why Is Obama Threatening Russia With World War 3 Right Before The Election? **The Economic Collapse**, San Franciso, California, August 21, 2018. October 21, 2016 Available at: http://theeconomiccollapseblog.com/archives/why-is-obama-threatening-russia-with-world-war-3-right-before-the-election.

SOLOMON, M. R. Groups and Social Media. *In*: (Ed.). **Consumer Behavior: Buying, Having, and Being**. 12th ed. London, United Kingdom: Pearson Education Limited, 2018. p. 414-445.

SOMAIYA, R. Donald Trump's wealth and poll numbers complicate news media's coverage. **The New York Times**, New York, July 24, 2015. Media. Available at: https://www.nytimes.com/2015/07/25/business/media/donald-trumps-wealth-and-poll-numbers-complicate-news-medias-coverage.html. Accessed on: April 22, 2019.

STARR, P.I Get Sanders' Appeal. But He's Not a Credible President. **Politico Magazine**, Virginia, n.Issue,2016a.

_____.Why Democrats should beware of Sanders' socialism. **Politico Magazine**, Virginia, n.Issue,2016b.

STEIN, J. A. Domesticity, Gender and the 1977 Apple II Personal Computer. **Design and Culture**, London, United Kingdom, v. 3, n. 2, p. 193–216, 2011.

STOLBERG, S. G.; N. FANDOS. Divided on impeaching Trump, Democrats wrestle with duty and politics. **The New York Times**, New York, April 24, 2019. Politics. Available at: https://www.nytimes.com/2019/04/24/us/politics/democrats-impeaching-trump-division.html. Accessed on: April 27, 2019.

STRASSMANN, P. A. **Information Payoff: The transformation of work in the electronic age**. New York: The Free Press, 1985.

STRATE, L. The varieties of cyberspace: Problems in definition and delimitation. **Western Journal of Communication**, v. 63, n. 3, p. 382–412, 1999.

STYLES, E. A. Attention, perception, and memory: An integrated introduction. *In*: (Ed.). New York, New York: Psychology Press, 2005.

_____. Automaticity, skill and expertise. *In*: (Ed.). **The Psychology of Attention**. 2nd. ed. New York, New York: Psychology Press, 2006. p. 183-214.

STYLIANIDIS, A. **Metaphors in user-interfaces design**. Birmingham, United Kingdom: University of Birmingham, 2015. Available at: https://pdfs.semanticscholar.org/fe80/67cde778efd8e8406e3a3fa24b0afb766979.pdf. Accessed on: August 23, 2018.

SUTHERLAND, A. **The story of Google** 1st. ed. New York, New York: The Rosen Publishing Group, Inc., 2012.

SZOLDRA, P. What constitutes a 'act of cyber war'? One senator wants to figure that out. **Business Insider**, New York, New York, June 16, 2016. Politics. Available at: https://www.businessinsider.com/what-is-an-act-of-cyber-war-2016-6. Accessed on: April 5, 2019.

TACOPINO, J. US prepped for massive cyber assault on Russia. **New York Post**, New York, New York, October 14, 2016. News. Available at: https://nypost.com/2016/10/14/us-prepped-for-massive-cyber-assault-on-russia/. Accessed on: May 14, 2019.

TALBOT, M. Trump and the Truth: The "lying" media. **The New Yorker**, New York, September 28, 2016. News & Poltics. Available at: https://www.newyorker.com/news/news-desk/trump-and-the-truth-the-lying-media. Accessed on: April 19, 2019.

TAMBINI, D. **Fake news: public policy responses**. The London School of Economics and Political Science. London, United Kingdom: SCIENCE, T. L. S. O. E. A. P., April 7, 2017. p. 1-16.

TANDOC, E. C. *et al.* Audiences' acts of authentication in the age of fake news: A conceptual framework. **New Media & Society**, Thousand Oaks, California, v. 20, n. 8, p. 2745-2763, 2018.

TANG, D. *et al.* Coooolll: A Deep Learning System for Twitter Sentiment Classification. *In*: Proceedings of the 8th International Workshop on Semantic Evaluation (SemEval 2014), 8. 2014, Dublin, Ireland. **Conference Paper.** Stroudsburg, Pennsylvania: Association for Computational Linguistics, 2014. p. 208-212. Available at: http://www.aclweb.org/anthology/S14-2033.

TENG, J. *et al.* **Determining a quality score for a content item** Applicant: GOOGLE LLC. Procurer: Junbin Teng, Anja Hauth, Alexander Sobol and Boris Mazniker. US9727644B1. Filing: September 25, 2013. Publication: August 8, 2017. Google Patents. Available at: https://patents.google.com/patent/US9727644B1. Accessed on: May 22, 2019.

THE WASHINGTON POST; ABC NEWS. **Washington Post-ABC News poll Jan. 21-24, 2019**. Washington, D.C.: Fred Ryan, 2019. Available at: https://www.washingtonpost.com/page/2010-2019/WashingtonPost/2019/01/25/National-Politics/Polling/release_539.xml. Accessed on: April 28, 2019.

THIELMAN, S. Chinese hack of US national security details revealed days after Russian hack. **The Guardian**, New York, August 10, 2015. World. Available at: https://www.theguardian.com/world/2015/aug/10/chinese-national-security-officials-hack. Accessed on: April 14, 2019.

TOMS, Y. *et al.* **A system and associated method for selecting advertisements**. Applicant: ALCATEL LUCENT SAS. Procurer: Axel Ivo Michel Plas. EP 1 990 762 A1. Filing: May 7, 2007. Publication: November 12, 2008. Google Patents. Available at: https://patents.google.com/patent/EP1990762A1/nl. Accessed on: April 20, 2019.

TOOSI, N.; S. M. KIM. **'Treason'? Critics savage Trump over Russia hack comments**. Politico. Arlington, Virginia: John F. Harris, 2016. Available at: https://www.politico.com/story/2016/07/trump-russia-clinton-emails-treason-226303. Accessed on: April 15, 2019.

TÖRNBERG, P.; A. TÖRNBERG. The limits of computation: A philosophical critique of contemporary Big Data research. **Big Data & Society**, Thousand Oaks, California, v. 5, n. 2, p. 1-12, 2018.

TOURANGEAU, R.; M. P. COUPER; D. M. STEIGER. Humanizing self-administered surveys: experiments on social presence in web and IVR surveys. **Computers in Human Behavior**, New York, New York, v. 19, n. 1, p. 1-24, 2003.

TRAPHAGEN, M. The Three Pillars of SEO: Authority, Relevance, and Trust. **Search Engine Journal**, Boca Raton, Florida, June 15, 2018. Complete Guide to SEO. Available at: https://www.searchenginejournal.com/seo-guide/search-authority/#close.

TRUMP, D. **Speech: Donald Trump - Colorado Springs, CO - October 18, 2016**: Factbase Videos, 2016. Available at: https://youtu.be/2BOXidI3798. Accessed on: April 19, 2019.

TRUMP, D. J. **Donald J. Trump:** Interview [June 2015] Interviewer: O'REILLY, B. New York, New York: Fox, 2015. 10min42s. Fox News' Bill O'Reilly interviews Donald Trump after his candidacy announcement

_____. **Presidential proclamation on declaring a national emergency concerning the southern border of the United States**. Washington, D.C.: The

White House, 2019. Available at: https://www.whitehouse.gov/presidential-actions/presidential-proclamation-declaring-national-emergency-concerning-southern-border-united-states/. Accessed on: April 27, 2019.

TURK, J. V. Information subsidies and influence. **Public Relations Review**, New York, New York, v. 11, n. 3, p. 10–25, 1985.

_____. Information subsidies and media content: a study of public relations influence on the news. **Journalism Monographs, 100**, Columbia, South Carolina, 1986.

U.S. BUREAU OF ECONOMIC ANALYSIS. **Private fixed investment, chained price index: Nonresidential: Equipment: Information processing equipment: Computers and peripheral equipment**. St. Louis, Missouri: Federal Reserve Bank of St. Louis, 2018. Available at: https://fred.stlouisfed.org/graph/?g=l1bQ.

UCHILL, J. Guccifer 2.0 releases new DNC docs. **The Hill**, Washington, D.C., July 13, 2016. Cybersecurity. Available at: https://thehill.com/policy/cybersecurity/287558-guccifer-20-drops-new-dnc-docs. Accessed on: April 6, 2019.

UNITED STATES. National Emergencies Act. War and National Defense. U.S. Code. 50 U.S.C. § 1601. 90 Stat. 1255. Pub. L. 94–412. **U.S. Government Publishing Office**, Washington, D.C., September 14, 1976. Available at: https://www.govinfo.gov/content/pkg/STATUTE-90/pdf/STATUTE-90-Pg1255.pdf. Accessed on: April 27, 2019.

_____. Construction authority in the event of a declaration of war or national emergency. Armed Forces. U.S. Code. 10 U.S.C. § 2808. 96 Stat. 157. Pub. L. 97–214. **U.S. Government Publishing Office**, Washington, D.C., July 12, 1982. Available at: https://www.govinfo.gov/content/pkg/USCODE-2010-title10/pdf/USCODE-2010-title10-subtitleA-partIV-chap169-subchapI-sec2808.pdf. Accessed on: April 27, 2019.

_____. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008. War and National Defense. U.S. Code. 50 U.S.C. § 1801. 122 Stat. 2436. Pub. L. 110–261. **U.S. Government Publishing Office**, Washington, D.C., July 10, 2008. Available at: https://www.govinfo.gov/content/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf. Accessed on: May 7, 2019.

_____. Executive Order 13660. March 6, 2014. **Blocking property of certain persons contributing to the situation in Ukraine**, Issued by BARACK OBAMA. Washington, D.C., v. 79, n. 46, p. 13491-13495, 2014a. Available at: https://www.federalregister.gov/documents/2014/03/10/2014-05323/blocking-property-of-certain-persons-contributing-to-the-situation-in-ukraine. Accessed on: April 25, 2019.

_____. Executive Order 13661. March 16, 2014. **Blocking property of additional persons contributing to the situation in Ukraine**, Issued by BARACK OBAMA. Washington, D.C., v. 79, n. 53, p. 15533-15538, 2014b. Available at: https://www.federalregister.gov/documents/2014/03/19/2014-06141/blocking-

property-of-additional-persons-contributing-to-the-situation-in-ukraine. Accessed on: April 25, 2019.

_____. Executive Order 13694 April 1, 2015. **Blocking the property of certain persons engaging in significant malicious cyber-enabled activities**, Issued by BARACK OBAMA. Washington, D.C., v. 80, n. 63, p. 18077-18079, 2015. Available at: https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities. Accessed on: April 25, 2019.

_____. U.S. Senate. Cyber Act of War Act of 2016, **Bill**. S.2905. To require the President to develop a policy for determining when an action carried out in cyberspace constitutes an act of war against the United States. Introduced by MIKE ROUNDS. Washington, D.C., May 9, 2016. Available at: https://www.rounds.senate.gov/imo/media/doc/Bill,%20NDAA%202017%20Related,%20Cyber%20Act%20of%20War.pdf. Accessed on: April 25, 2019.

_____. U.S. House of Representatives. Cyber Act of War Act of 2016, **Bill**. H.R.5220. To direct the President to develop a policy on when an action in cyberspace constitutes a use of force against the United States. Introduced by JAMES A. HIMES. Washington, D.C., May 12, 2016. Available at: https://www.congress.gov/114/bills/hr5220/BILLS-114hr5220ih.pdf. Accessed on: April 25, 2019.

_____. Executive Order 13757. December 28, 2016. **Taking additional steps to address the national emergency with respect to significant malicious cyber-enabled activities**, Issued by BARACK OBAMA. Washington, D.C., v. 82, n. 1, p. 1-3, 2016c. Available at: https://www.federalregister.gov/documents/2017/01/03/2016-31922/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious. Accessed on: April 25, 2019.

_____. Executive Order 13780. March 6, 2017. **Protecting the Nation From Foreign Terrorist Entry Into the United States**, Issued by DONALD J. TRUMP. Washington, D.C., v. 82, n. 45, p. 13209-13219, 2017. Available at: https://www.federalregister.gov/documents/2017/03/09/2017-04837/protecting-the-nation-from-foreign-terrorist-entry-into-the-united-states. Accessed on: April 30, 2019.

_____. U.S. Congress. Joint Resolution relating to a national emergency declared by the President on February 15, 2019, **Joint Resolution**. H.J.Res.46. Resolved by the U.S. Congress that the national emergency declared by the President on February 15, 2019 is hereby terminated. Introduced by NANCY PELOSI. Washington, D.C., February 22, 2019. Available at: https://www.congress.gov/116/bills/hjres46/BILLS-116hjres46enr.pdf. Accessed on: April 27, 2019.

VALERIANO, B.; R. C. MANESS. International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain. *In*: BROWN, C. e ECKERSLEY, R. (Ed.). **The Oxford Handbook of International Political Theory**. Oxford, United Kingdom: Oxford University Press, 2018. p. 259-272.

VARGO, C. J.; L. GUO; M. A. AMAZEEN. The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016. **New Media & Society**, Thousand Oaks, California, v. 20, n. 5, p. 2028-2049, 2017.

VÁZQUEZ, S. *et al.* A classification of user-generated content into consumer decision journey stages. **Neural Networks**
New York, New York, v. 58, p. 68-81, 2014.

VELDE, J. V. D. The Law of Cyber Interference in Elections. **Social Science Research Network**, New York, New York, p. 1-39, 2016.

VERTELNEY, L. J. *et al.* **User interface system having programmable user interface elements**. Applicant: APPLE COMPUTER, I. Procurer: Laurie J. Vertelney, Thomas D. Erickson, S. Joy Mountford, John J. Thompson-Rohrlich, Gitta B. Salomon, Yin Y. Wong, Daniel S. Venolia, Kathleen M. Gomoll, Eric A. Hulteen. US5202828A. Filing: May 15, 1991. Publication: April 13, 1993. Google Patents. Available at: https://patents.google.com/patent/US5202828A. Accessed on: May 22, 2019.

VICENS, A.DNC Hacker Dumps Trove of Clinton Documents. **Mother Jones**, San Francisco, n.Issue,2016.

VICIOSO, S. **Programmatic Advertising 101: How It Works** Seer. San Diego, California: Seer Interactive, 2015a. Available at: https://www.seerinteractive.com/blog/programmatic-advertising-101-works/. Accessed on: May 18, 2019.

_____. **Programmatic Buying: Simple Guide to Get You Started** Seer. San Diego, California: Seer Interactive, 2015b. Available at: https://www.seerinteractive.com/blog/programmatic-guide/. Accessed on: May 18, 2019.

VIJAYARAGHAVAN, R.; K. M. ADUSUMILLI; P. V. KANNAN. **Ad-words optimization based on performance across multiple channels**. Applicant: 24/7 CUSTOMER INC. Procurer: Ravi Vijayaraghavan, Kranthi Mitra Adusumilli and Pallipuram V. Kannan. US20140156383A1. Filing: November 27, 2013. Publication: June 5, 2014. Google Patents. Available at: https://patents.google.com/patent/US20140156383A1. Accessed on: May 19, 2019.

VISE, D. A. **The Google Story**. London, United Kingdom: Pan Books, 2006.

VITALARI, N. P.; A. VENKATESH; K. GRONHAUG.Computing in the home: shifts in the time allocation patterns of households. **Communications of the ACM**, New York, New York, v. 28, n.Issue, p. 512-522,1985.

VOLZ, D.; J. MENN.Russian Hackers Stole U.S. Cyber Secrets From NSA: Media Reports. **U.S. News & World Report**, New York, New York, n.Issue,2017.

VOLZ, D.; E. STEPHENSON. Russians steal research on Trump in hack of U.S. Democratic Party. **Reuters**, London, June 14, 2016. Politics. Available at:

https://www.reuters.com/article/us-usa-election-hack-idUSKCN0Z0205. Accessed on: April 15, 2019.

VOSOUGHI, S.; P. VIJAYARAGHAVAN; D. ROY. Automatic detection and categorization of election-related Tweets. *In*: Proceedings of the Tenth International AAAI Conference on Web and Social Media, 10. 2016, Cologne, Germany. **Conference Paper.** Menlo Park, California: Association for the Advancement of ArtificialIntelligence, 2016. p. 703-706. Available at: https://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13159. Accessed on August 2, 2018.

VOSOUGHI, S. *et al.* Mapping Twitter conversation landscapes. *In*: Proceedings of the Eleventh International AAAI Conference on Web and Social Media, 11. 2016, Montreal, Canada. **Conference Paper.** Menlo Park, California: Association for the Advancement of Artificial Intelligence, 2016. Accessed on May 22, 2019.

VOSOUGHI, S. *et al.* **The Electome**. Cambridge, Massachusetts. Available at: http://electome.org/. Accessed on: August 24.

WAISBORD, S. Truth is what happens to news: On journalism, fake news, and post-truth. **Journalism Studies**, London, United Kingdom, v. 19, n. 13, p. 1866-1878, 2018.

WAISBORD, S.; T. TUCKER; Z. LICHTENHELD. Trump and the great disruption in public communication. *In*: BOCZKOWSKI, P. J. e PAPACHARISSI, Z. (Ed.). **Trump and the media**. Cambridge, Massachussetts: MIT Press, 2018. p. 25-32.

Cyber-enabled Information Operations: **Hearings before the Senate Armed Services Committee, Subcommittee on Cybersecurity**, U.S. Senate, 115th Congress.The Weaponization of Information: The need for cognitive security (Rand Waltzman), p. 1-8, 2017.

WANG, Y. *et al.* Unsupervised sentiment analysis for social media images. *In*: Proceedings of the Twenty-Fourth International Joint Conference on Artificial Intelligence, 24. 2015, Buenos Aires, Argentina. **Conference Paper.** Palo Alto, California: Association for the Advancement of Artificial Intelligence, 2015. Accessed on May 22, 2019.

WASHINGTON (STATE). United States Court of Appeals for the Ninth Circuit. **Opinion**. 440 Other Civil Rights. Violation of 5th & 8th Amendments. 28 U.S.C. § 1331. Plaintiffs: State of Hawaii and Ismail Elshikh. Defendants: Donald J. Trump, John F. Kelly and Rex W. Tillerson. Judge: DERRICK K. WATSON. Submitted: Seattle, Washington, May 15, 2017. United States Court of Appeals for the Ninth Circuit: Seattle, Washington, 17-15589, June 12, 2017. Available at: http://cdn.ca9.uscourts.gov/datastore/opinions/2017/06/12/17-15589.pdf. Accessed on: April 30, 2019.

_____ (DISTRICT OF COLUMBIA). United States District Court for the District of Columbia. **Indictment**. Conspiracy to commit offense or to defraud the United States, Attempt and conspiracy, Aggravated identity theft. 18 U.S.C. §§ 2, 371, 1349, 1028A.

Plaintiffs: United States of America. Defendants: Internet Research Agency, et al. Judge: DABNEY FRIEDRICH. Submitted: Washington, D.C., February 16, 2018. U.S. Department of Justice: Washington, D.C., 1:18-cr-00032-DLF, February 16, 2018. Available at: https://www.justice.gov/file/1035477/download. Accessed on: August 22, 2018.

_____ (DISTRICT OF COLUMBIA). United States District Court for the District of Columbia. **Indictment**. Conspiracy to commit offense or to defraud United States, Attempt and conspiracy, Aggravated identity theft, Laundering of monetary instruments. 18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, 3551. Plaintiffs: United States of America. Defendants: Viktor Borisovich Netyksho, et al. Submitted: Washinton, D.C., July 13, 2018. U.S. Department of Justice: Washinton, D.C., 1:18-cr-215, July 13, 2018. Available at: https://www.justice.gov/file/1080281/download. Accessed on: August 22, 2018.

WATTS, D. J.; D. M. ROTHSCHILD.Don't blame the election on fake news. Blame it on the media. **Columbia Journalism Review**, New York, New York, n.Issue,2017.

WEBER, M. **Economy and Society: An outline of interpretive sociology**. Berkeley: University of California Press, 1978.

WEISSMAN, A. J.; G. I. ELBAZ. **Meaning-based advertising and document relevance determination** Applicant: GOOGLE LLC. Procurer: Adam J Weissman and Gilad Israel Elbaz. US7698266B1. Filing: March 24, 2004. Publication: April 13, 2010. Google Patents. Available at: https://patents.google.com/patent/US7698266B1. Accessed on: May 22, 2019.

WHEELER, S. MBA Tech: New privacy laws pose looming threat to lenders. **HousingWire.com**, Irving, Texas, March 26, 2019. Lending. Available at: https://www.housingwire.com/articles/48559-mba-tech-new-privacy-laws-pose-looming-threat-to-lenders. Accessed on: March 27, 2019.

WINSTON, B. **Media Technology and Society: A History : From the Telegraph to the Internet**. New York: Routledge, 1998.

Why we're living in the age of fear. Politics Features. **Rolling Stone**. October 6, 2016. 1min43s. Available at: http://www.rollingstone.com/politics/features/why-were-living-in-the-age-of-fear-w443554. Accessed on May 28, 2019.

WOLFERS, J.; E. ZITZEWITZ. What do financial markets think of the 2016 election? **Brookings**, Washington, D.C., October 20, 2016. Research. Available at: https://www.brookings.edu/wp-content/uploads/2016/10/what-do-financial-markets-think-of-the-2016-election_102016_wolferszitzewitz.pdf. Accessed on: May 28, 2019.

WORLD WIDE WEB CONSORTIUM. **Resource Description Framework (RDF) Model and Syntax Specification**. Cambridge, Massachusetts, January 5, 1999. Available at: http://www.w3.org/TR/1999/PR-rdf-syntax-19990105. Accessed on: May 23, 2019.

YAN, J. *et al.* **Semantic user profiles for targeting user segments**. Applicant: MICROSOFT TECHNOLOGY LICENSING LLC. Procurer: Jun Yan, Ning Liu, Lei Ji, Steven J. Hanks, Qing Xu and Zheng Chen. US9098541B2. Filing: September 6, 2013. Publication: August 4, 2015. Google Patents. Available at: https://patents.google.com/patent/US9098541B2. Accessed on: May 19, 2019.

YANG, S.; E. HOLODNY. The Massive Hack Of The Nasdaq That Has Wall Street Terrified Of Cyber Attacks. **Business Insider**, New York, New York, June 17, 2014. Available at: https://www.businessinsider.com/nasdaq-attacked-by-hackers-2014-7. Accessed on: April 13, 2019.

YGLESIAS, M. It's time for Bernie Sanders to admit he lost and drop out. **Vox**, Washington, D.C., June 7, 2016. Politics & Policy. Available at: https://www.vox.com/2016/6/7/11878108/bernie-sanders-lost. Accessed on: April 11, 2019.

ZAMANZADEH, B.; J. STEPHEN JOHN ZIMMERMAN; C. RAMAKRISHNAN. **Systems and methods for the semantic modeling of advertising creatives in targeted search advertising campaigns** Applicant: DATAPOP INC. Procurer: John Zimmerman, Behzad Zamanzaden, Swaranjit Dua and John Warden. US9972030B2. Filing: March 11, 2013. Publication: May 15, 2018. Google Patents. Available at: https://patents.google.com/patent/US9972030B2. Accessed on: May 19, 2019.

ZHAO, G.; P. FU. **System and method for ad keyword scoring** Applicant: GOOGLE LLC. Procurer: Gaofeng Zhao and Ping Fu. US9406077B1. Filing: October 19, 2011. Publication: August 2, 2016. Google Patents. Available at: https://patents.google.com/patent/US9406077B1. Accessed on: May 22, 2019.

ZHAO, J.; M. LAN; T. ZHU. Expression- and message-level sentiment orientation classification in Twitter using multiple effective features. *In*: Proceedings of the 8th International Workshop on Semantic Evaluation (SemEval 2014), 8. 2014, Dublin, Ireland. **Conference Paper.** Stroudsburg, Pennsylvania: Association for Computational Linguistics, 2014. p. 259-264 Available at: http://www.aclweb.org/anthology/S14-2042. Accessed on August 2, 2018.

ZHU, H. *et al.* Towards expert finding by leveraging relevant categories in authority ranking. *In*: CIKM '11 Proceedings of the 20th ACM international conference on Information and knowledge management, 11. 2011, Glasgow, Scotland. **Conference Paper.** New York, New York: Asssociation for Computing Machinery, 2011. p. 2221-2224.

ZIMMERMAN, J. *et al.* **Semantic model based targeted search advertising**. Applicant: DATAPOP INC. Procurer: John Zimmerman, Behzad Zamanzaden, Swaranjit Dua and John Warden. US20140258002A1. Filing: March 11, 2013. Publication: September 11, 2014. Google Patents. Available at: https://patents.google.com/patent/US20140258002A1. Accessed on: May 19, 2019.